D51 / 03.06-05 17.10.2019

Antworten auf die Fragen der Handelskammer Hamburg

Frage 1: Kann eine Black- und eine Whitelist für die Datenschutzfolgenabschätzung zur Verfügung gestellt werden, und ggfs. wann kann dies erfolgen?

Die sogenannte Blacklist ist auf unserer Internetseite abrufbar.[1] Weder auf deutscher noch auf europäischer Ebene sind Bestrebungen erkennbar, eine sogenannte Whitelist zu verabschieden. Insofern beabsichtigen wir auch keine Erstellung einer Whitelist, weil ein Hamburger Alleingang für die Rechtssicherheit insgesamt nicht hilfreich wäre.

Frage 2: Welchen Anpassungs-/Änderungsbedarf bzgl. Cookie Policy Hinweisen erwartet die DS-Behörde von unternehmen / ab wann ist die Erforderlichkeit eines Cookies oder eine technische Lösung i.S.d. Abs. 1 lit. f) gegeben (bspw. Integragtion von Social Feeds und Videos, die andernfalls nicht dargestellt werden könnten)?

Die DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) hat eine Position „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“ veröffentlicht.[2] Danach sind auch für die Datenverarbeitung des Trackings (realisiert etwa durch Cookies, aber auch andere technische Möglichkeiten sind üblich) die Maßstäbe der DSGVO anzuwenden. Als Rechtsgrundlage kommen die in Art 6 DSGVO genannten Fälle in Betracht. Abhängig von der Funktion des Cookies kann hier sowohl Vertragserfüllung, Einwilligung wie auch berechtigtes Interesse in Frage kommen. Die verschiedenen Cookies bzw. anderen Techniken sollten entsprechend gekennzeichnet werden und dort, wo nur die Einwilligung in Betracht kommt, erst dann verwendet werden, wenn eine solche Einwilligung vorliegt.

Frage 3: Datenportabilität: Fallen auch Mitarbeiterdaten hierunter?

Ja, aber nur soweit die betreffenden Daten auf Grundlage einer Einwilligung oder eines Vertrags nach Art. 6 Abs. 1 lit. b DSGVO beruht (siehe Art. 20 DSGVO). Das trifft in der Praxis auf Mitarbeiterdaten nur selten zu, da diese in der Regel auf Grundlage von § 26 Abs. 1 BDSG verarbeitet werden.

Frage 4: Wie sind die Informationen nach Art. 13 DSGVO mitzuteilen bei Visitenkarten, E-Mail-Austausch und Call Centern bei erstmaligem Kontakt – reichen Verweise auf eine Internetseite aus, auf der die Infos bereit gehalten werden?

Die Informationspflichten lösen in verschiedenen Konstellationen immer wieder Fragen aus, die keinesfalls pauschal mit dem Verweis auf eine Internetseite beantwortet werden können.

[1] https://datenschutz-hamburg.de/dsgvo-information/art-35-mussliste-nicht-oeffentlich/
[2] https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf

Wie Kurzpapier Nr. 10 der Aufsichtsbehörden ausgeführt,[3] müssen bei der **Direkterhebung** die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden. Darüber hinaus enthält das Kurzpapier angesichts der Vielzahl von Möglichkeiten keine Hinweise, wie in Einzelfällen genau zu verfahren ist. Insgesamt gibt es hierzu sehr unterschiedliche Meinungen, die sich weiterhin in lebhafter Diskussion befinden. Gleichwohl möchten wir Ihnen zu den angeführte Einzelfällen mitteilen, wie wir uns mögliche Lösungen vorstellen. Wie bei allen hier zu beantwortenden Fragen steht dies unter dem Vorbehalt anderweitiger neuer Erkenntnisse:

- Bei der Entgegennahme von Visitenkarten fallen zwar sofort personenbezogene Daten an, gleichwohl wird die Informationspflicht nicht unmittelbar ausgelöst. Solange eine Visitenkarte angenommen und eingesteckt wird, erfolgt noch keine Verarbeitung personenbezogener Daten, da weder eine automatisierte, noch eine nichtautomatisierte Verarbeitung stattfindet. Der sachliche Anwendungsbereich der DSGVO ist also nicht ausgelöst (Art. 2 Abs. 1 DSGVO). Erst, wenn diese Daten in eine Datei aufgenommen werden, beginnt die Anwendbarkeit der DSGVO. Nun könnte man trefflich darüber streiten, ob diese dateimäßige Verarbeitung der bereits im Vorfeld erhobenen Daten noch als Erhebung personenbezogener Daten im Sinne des Art. 13 DSGVO angesehen werden kann, ob – wenn die nachträgliche dateimäßige Verarbeitung zum Zeitpunkt der Erhebung schon absehbar war – die Informationspflicht doch schon früher ausgelöst wurde oder ob eine solche Verwendung der Visitenkarten dann vielleicht sogar unzulässig ist. In der Praxis muss es jedoch möglich sein, die Informationspflichten bei Aufnahme in eine Datei nachzuholen. Alle anderen Fälle unterliegen ihr sowieso nicht. Mit der nachträglichen und schnellstmöglichen Information der Betroffenen, die gesetzlich auch die Hinweise auf das Recht auf Löschung und Widerspruch (Art. 13 Abs. 2 lit.b DSGVO) enthält, ist es empfehlenswert, gerade diese Rechte noch einmal besonders herauszustellen. Damit sollte dem Betroffenen noch einmal die Freiwilligkeit, die ja mit der Herausgabe der Visitenkarte verbunden war, deutlich gemacht werden. Möglicherweise hatte er zu dem Zeitpunkt auch nicht mit einer dateimäßigen Verarbeitung gerechnet und sollte sie schnell und folgenlos rückgängig machen können.
- Hinsichtlich des E-Mail-Austausches verweisen wir auf die Transparency-Guidelines, WP 260.[4] Dort gibt es Hinweise unter Rz. 17.
- Im Bereich der Informationspflichten durch Call-Center gibt es noch große Unsicherheiten. Zwar kann man auch hier davon ausgehen, dass andere als schriftliche Formen der Information möglich sind und (dann: mündliche) Hinweise auf Webseiten in vielen Fällen die Verpflichtungen erfüllen können. Gleichwohl müssen jedenfalls gewisse Grundinformationen bereits bei oder vor dem Gespräch mündlich erteilt werden. Über diese hinaus kann auf einen Text im Internet verwiesen werden. Fall aber der Gesprächspartner sofortige Informationen möchte, weil er beispielsweise nicht über einen Internetanschluss verfügt, müssen Ihm die Informationen vom Call-Center-Agent mitgeteilt werden.

Frage 5: Wie sind Informationen nach Art. 14 DSGVO mitzuteilen? Wann sind sie mitzuteilen, wenn diese Daten beiläufig erhoben werden (z.B. Auflistung neuer Eventlocations und Bars die eröffnen und Recherche der Kontaktinformationen)?

Hinsichtlich der Recherche von Kontaktinformationen muss zunächst sichergestellt werden, dass es dafür eine Rechtsgrundlage gibt. Sollte das der Fall sein, gibt es hinsichtlich der Informationspflichten nach Art. 14 DSGVO keine Besonderheiten. Wenn ohnehin eine werbliche Ansprache der Kontakte erfolgt, spricht auch rein praktisch nichts dagegen, Datenschutzinformationen mitzusenden.

[3] https://datenschutz-hamburg.de/assets/pdf/DSK_Kurzpapier_Nr_10_Informationspflichten.pdf
[4] https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf

Frage 6: Der DDV (Deutscher Dialogmarketing Verband) vertritt die These, dass es wichtig ist, Daten aus öffentlich zugänglichen Quellen für Zwecke des Dialogmarketings und der Akquise zu zutzen. Ist dies aus Sicht des HmbBfDI zulässig?

Die Verwendung von Adressdaten für die Zusendung von Werbepost ist in vielen Fällen ohne Einwilligung der Empfänger zulässig. So ist die Briefwerbung an eigene Kunden grundsätzlich erlaubt, solange dem nicht widersprochen wurde. Darüber hinaus dürfen für die Neukundenwerbung Adressen eines Dritten genutzt werden (beispielsweise aus dem Telefonbuch, aus einem Adressbuch oder von einem Adressverlag). In diesem Fall muss zur Erfüllung der Informationspflichten aus der Werbung hervorgehen, wo die Adresse herstammt. Auch eine Verarbeitung von Postadressdaten für Zwecke der eigenen Direktwerbung aus der Durchführung von Preisausschreiben und Gewinnspielen sowie aufgrund von Katalog- und Prospektanforderungen ist nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO zulässig, wenn über die werbliche Datenverarbeitung informiert wurde; eine Einwilligung der betroffenen Personen ist bei solchen Sachverhalten dann nicht erforderlich.

Nicht zulässig ist hingegen das Auslesen der Daten aus einem Online-Impressum zum Zweck der werblichen Nutzung. Zwar sind diese Daten allgemein zugänglich, sie werden jedoch nicht freiwillig, sondern aufgrund der gesetzlichen Verpflichtung zur Anbieterkennzeichnung gem. § 5 TMG bzw. § 55 Abs. 2 RStV veröffentlicht. Mangels Freiwilligkeit der Veröffentlichung führt die Interessenabwägung gem. Art. 6 Abs. 1 lit. f DSGVO regelmäßig dazu, dass die werbliche Nutzung so erhobener Daten unzulässig ist. Insofern verbietet sich eine allgemein gültige Aussage im Hinblick auf die Zulässigkeit einer werblichen Nutzung von Daten aus allgemein zugänglichen Quellen.

Frage 7: In den Regelungen zur Auftragsdatenverarbeitung (Art. 28 DSGVO) steht nicht nur, dass man einen Vertrag braucht. Es steht dort auch, dass man den Auftragnehmer überprüfen sollte. Überspitzt gesagt müsste ein Unternehmer, der Google Analytics nutzt, dann nach Irland fahren und eine Überprüfung bei Google durchführen. Absatz 3 Ziffer h spricht hier von Inspektionen. Wie sieht das praktisch aus? Wer muss aktiv werden?

Diese Vorschrift weicht nicht wesentlich vom alten Recht ab, wonach in dem Vertrag „ die Kontrollrechte des Auftraggebers und die entsprechende Duldungs- und Mitwirkungspflicht des Auftragnehmers“ zu regeln war (§ 11 Abs. 2 Nr. 7 BDSG-alt). Auch in Art. 28 Abs. 3 lit. h) DSGVO ist lediglich von den Überprüfungsrechten des Auftraggebers die Rede, die der Auftragnehmer ermöglichen muss. Insofern hat sich wenig geändert. Hintergrund ist die Tatsache, dass im Falle der Auftragsverarbeitung in jedem Fall der Auftraggeber verantwortlich bleibt und die Möglichkeit haben muss, bei Zweifeln oder auch weil es seinem Selbstverständnis von Verantwortung entspricht, Kontrollen bei dem Auftragnehmer vorzunehmen. Bei großen IT-Dienstleistern ist es nachvollziehbar, wenn diese schon aus Gründen der Datensicherheit nicht jedem Kunden Zugang zu ihren Serverräumen gewähren möchten. In der Praxis wird dieses Spannungsverhältnis in der Regel durch Zertifizierungen aufgelöst. Die einzelnen Auftraggeber bedienen sich dann eines gemeinsamen Kontroll-Dienstleisters, der stellvertretend für sie Vor-Ort-Kontrollen durchführt.

Frage 8: Wonach richtet sich die Zuständigkeit der federführenden Auchsichtsbehörde gemäß Art. 56 DSGVO für eine konzernweite (selbständige Töchter – kein Netz von Niederlassungen) und länderübergreifende (innerhalb der EU) Datenverarbeitung? Erfolgt die Meldung z.B. von Datenschutzverstößen dann nur an diese eine Aufsichtsbehörde? Wie ist generell mit Anfragen ausländischer Aufsichtsbehörden umzugehen.

Die Zuständigkeit der federführenden Aufsichtsbehörde für eine in Europa ansässige Konzerntochter richtet sich nach ihrem Sitz. Die länderübergreifende Datenverarbeitung kann dazu füh-

ren, dass die Aufsichtsbehörden untereinander das Kohärenzverfahren einleiten. Zur Meldung an die richtige Aufsichtsbehörde kann auf WP 250[5] und dort auf den Punkt „ Breaches affecting individuals in more than one Member State“ (S. 14 f.) verwiesen werden. Zum generellen Umgang mit Anfragen ausländischer Aufsichtsbehörden kommt es auf den jeweiligen Einzelfall an: Sofern es sich um Anfragen aus Drittländern handelt, haben die europäischen Aufsichtsbehörden darauf keinen direkten Einfluss. Hier ist zu beachten, dass die Vorschriften der DSGVO eingehalten werden müssen. In Zweifelsfällen sollte die zuständige Aufsichtsbehörde um Rat gefragt werden. Im Falle von Anfragen einer europäischen, jedoch unzuständigen Aufsichtsbehörde sollte mit der zuständigen Aufsichtsbehörde Rücksprache genommen werden.

Frage 9: Bezug nehmend auf das Urteil des EuGH vom 5. Juni 2018 stellt sich die Frage des Umgangs mit Facebook Fanpages. Ein zeitnaher Abschluss eines Joint Controller Agreements scheint nicht möglich. Gibt es Alternativen zur Abschaltung von Fanpages?

Die von Facebook mittlerweile zur Verfügung gestellte Vereinbarung nach Art 26 DSGVO wird von den Datenschutzaufsichtsbehörden in Deutschland und Europa aktuell geprüft. Es bestehen erhebliche Zweifel, dass diese Vereinbarung die Anforderungen von Art 26 DSGVO vollständig erfüllt.
Leider bietet Facebook nach unserer Kenntnis weiterhin dem Fanpage-Betreiber nicht die Möglichkeit an, die Erfassung der Besucherzahlen und anderer Nutzungsinformationen zu deaktivieren. Dies wäre eine Alternative zur Abschaltung der Page.

Frage 10: Wie ist mit Anfragen öffentlicher Stellen umzugehen (Polizei, Staatsanwaltschaft, weitere behördliche Anfragen)? Wie ist das Verhältnis DSGVO zu nationalen Gesetzen im Hinblick auf Auskunftsersuchen?

Die DSGVO erlaubt die Datenweitergabe an staatliche Stellen, wenn nationales Recht eine Verpflichtung zur Herausgabe vorsieht (Art. 6 Abs. 1 lit. c, Abs 2-3 DSGVO). Die Polizei/Staatsanwaltschaft/Datenschutzbehörde o.ä. kann damit auf Grundlage des Polizeirechts/der StPO/des BDSG Daten herausverlangen. Diese dürfen und müssen dann übermittelt werden. Voraussetzung ist, dass die Behörde die nationale Vorschrift korrekt geprüft hat. Wenn erkennbar ist, dass die Behörde rechtswidrig handelt, darf keine Datenübermittlung stattfinden. Dasselbe gilt, wenn es sich bei der nationalen Herausgabevorschrift um eine unverhältnismäßige Regelung gemäß Art. 6 Abs. 2 DSGVO handelt.

Frage 11: In welchem Anwendungsverhältnis stehen KUG und DSGVO? Inwieweit findet das KUG auf die Verarbeitung von Fotografien Anwendung?

Zu diesem Thema haben einen ausführlichen Vermerk gefertigt.[6] Im Ergebnis kann es dahinstehen, ob das KUG Anwendbarkeit findet, weil es ohnehin nur eine Rechtsgrundlage für die Veröffentlichung der Bilder enthält, während regelmäßig bereits die Datenerhebung mittels des Fotoapparats das Problem ist. Wir sehen für Fotografien in der Regel eine taugliche Rechtsgrundlage in Art. 6 Abs. 1 lit. f DSGVO, wobei wir die inhaltlichen Wertungen des KUG in die Interessenabwägung des Art. 6 Abs. 1 lit. f DSGVO einbeziehen.

Frage 12: Hinsichtlich der Datenportabilität stellt sich insbesondere die Frage, ob sich ein Anspruch auf Einsichtnahme in die Personalakte und Herausgabe aus den rechtlichen Ansprüchen der DSGVO oder arbeitsrechtlichen Vorschriften ergibt.

Da eine Personalakte in der Regel auf Grundlage von § 26 Abs. 1 BDSG geführt wird, unterfällt sie nicht dem Anspruch auf Datenportabilität gemäß Art. 20 DSGVO (siehe dazu Frage 3). Die

[5] https://datenschutz-hamburg.de/working-papers/wp-250/
[6] https://www.filmverband-suedwest.de/wp-content/uploads/2018/05/Vermerk_DSGVO.pdf

Frage stellt sich jedoch hinsichtlich des Anspruchs auf Herausgabe einer Kopie nach Art. 15 Abs. 3 DSGVO unterfällt. Auch der Beschäftigte hat ein Recht auf Herausgabe seiner in der Personalakte aufbewahrten personenbezogenen Daten. Das umfasst nicht notwendigerweise den gesamten Personalakteninhalt, insbesondere nicht alle Schriftstücke in vollständiger Form, sondern eine Abschrift der personenbezogenen Daten innerhalb der Schriftstücke. Da aber fast alle Daten in der Personalakte personenbezogen sind, ist es in der Praxis für gewöhnlich das Einfachste, den vollständigen Akteninhalt zu kopieren und zu übersenden. Dabei ist dann darauf zu achten, eventuelle Daten Dritter zu schwärzen.

Frage 13: Zum Thema „Meldung von Verletzung personenbezogener Daten an die Aufsichtsbehörde“ gem. Art. 33 DSGVO: Im Massengeschäft bei der Versendung von Post kann es zu „falschen Zustellungen“ kommen z.B. aufgrund von

- **Fehlerhaften Adressermittlungen (denkbar sind Namensgleichheiten),**
- **Fehlerhaften Kuvertierungen**
- **Fehlern im Rahmen der Postzustellung**

Dabei liegen die eigentlichen Fehler regelmäßig bei Dienstleistern in Auftagsverarbeitung oder der Post begründet und finden eher selten bei den Unternehmen hausintern statt. Die Folge kann jedoch sein, dass ein Dritter unzulässig von den personenbezogenen Daten eines anderen Kunden Kenntnis erlangt. Es handelt sich um Einzelfälle, jedoch im Massengeschäft durchaus einige Fälle. Auch bei hohen Sorgfaltsmaßstäben lassen sich diese Fälle nicht völlig vermeiden. Sollen dem Landesdatenschutzbeauftragten falsch versendete Briefe als Datenschutzverletzung gemeldet werden? Oder wollte der Gesetzgeber die klassischen (großen) Datenschutzpannen erfassen und hat dieses Massenphänomen der falschen Briefzustellung nicht gemeint?

Zu diesem Themenkomplex haben wir kürzlich eine ausführliche Handreichung herausgegeben.[7] Darin haben wir uns der Auffassung der europäischen Artikel-29-Gruppe angeschlossen,[8] wonach auch Fälle der versehentlichen Fehlversendung meldepflichtige Data Breaches sind. Wie in allen anderen Fällen auch besteht eine Meldepflicht bei Fehlversendungen jedoch nur dann, wenn aus dem Vorfall ein Risiko für die Rechte und Freiheiten der Betroffenen folgt. Ob dies der Fall ist, hängt von einer Einzelfallbetrachtung ab. Wesentliche Rolle dabei spielen die Sensibilität der im Brief enthaltenen Daten sowie die Anzahl der betroffenen Personen. Bei fehlerhaften Adressermittlungen und Kuvertierungen ist eine Meldung vom Verantwortlichen abzusetzen, also im Fall der Auftragsverarbeitung durch den Auftraggeber. Bei Fehlern im Rahmen der Postzustellung ist der Versanddienstleister zur Meldung verpflichtet, nicht der Absender. Für die Aufsicht über Versanddienstleister ist allerdings der Bundesdatenschutzbeauftrage ausschließlich zuständig, sodass auch nur dieser eine verbindliche Aussage zu deren Pflichten treffen kann.

[7] https://datenschutz-hamburg.de/assets/pdf/2018.11.15_Data%20Breach_Vermerk_extern.pdf
[8] https://datenschutz-hamburg.de/assets/pdf/wp250rev01_enpdf.pdf; dort auf S. 32 f.

Hamburg
Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO

für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen **im nicht-öffentlichen Bereich** durchzuführen ist

Stand: 17.10.2018
Version 1.1

A Gesetzliche Grundlage

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (EU-Datenschutz-Grundverordnung – DS-GVO) regelt im Abschnitt 3 „Datenschutz-Folgenabschätzung und vorherige Konsultation" des Kapitels IV „Verantwortlicher und Auftragverarbeiter" die Rahmenbedingungen zur sog. Datenschutz-Folgenabschätzung (kurz: DSFA; im Englischen Data Protection Impact Assessment oder DPIA). Artikel 35 DS-GVO nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Artikel 36 DS-GVO beschreibt das besondere Verfahren der Konsultation des Verantwortlichen bei der Aufsichtsbehörde bei Fortbestehen hoher Risiken auch nach Anwendung der auf Grundlage der DSFA festgelegten verhältnismäßigen technischen und organisatorischen Maßnahmen.

Grundlage dieses Dokuments ist Art. 35 Abs. 4 DS-GVO:

> *„Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss."*

Die vorliegende unter den Mitgliedern der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) abgestimmte Liste beinhaltet ausschließlich Verarbeitungsvorgänge aus dem nichtöffentlichen Bereich, darunter auch solche, die mit dem Angebot von Waren und Dienstleistungen für betroffene Personen in mehreren Mitgliedsstaaten verbunden sind. Sie unterliegt daher aufgrund von Art. 35 Abs. 6 DS-GVO dem Kohärenzverfahren gemäß Art. 63 DS-GVO.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in Art. 35 Abs. 3 DS-GVO oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DS-GVO von ihren Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO einschließlich der Verhängung von Geldbußen gemäß Art. 83 Abs. 4 DS-GVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DS-GVO offen.

Die in dem Dokument dargestellte Liste wird nachfolgend als „**Muss-Liste**" bezeichnet – gängige Begriffe in anderen Ländern sind hierfür auch „Blacklist" und „Positivliste".

B Ziel dieses Dokuments

Ziel des Dokuments ist es, einen Entwurf für die Liste nach Art. 35 Abs. 4 DS-GVO zu entwickeln, der auch auf europäischer Ebene diskutiert und nach Art. 35 Abs. 6 DS-GVO im Kohärenzverfahren gemäß Art. 63 DS-GVO behandelt werden kann, sofern die Bedingungen hierzu erfüllt sind. Berücksichtigt werden bisherige Veröffentlichungen von anderen Aufsichtsbehörden und Fachgremien, insbesondere das Working Paper 248 rev.01 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"" der Art. 29 Datenschutzgruppe sowie die umfangreichen internen Kommentierungen im Rahmen der UAG DSFA.

Das Dokument hat nicht den Anspruch der Vollständigkeit, wenngleich versucht wird, möglichst viele der DSFA-pflichtigen Verarbeitungsvorgänge zu berücksichtigen. Auf Grund der Schnelllebigkeit im digitalen Umfeld kann dieses Dokument nur als „lebendiges" Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungen in die Liste der Verarbeitungsvorgänge unterliegt. Die DSK wird hierfür einen Prozess erarbeiten, wie Verarbeitungstätigkeiten für die Muss-Liste vorschlagen, beurteilt und aufgenommen werden. Änderungen an Einträgen der Muss-Liste werden dokumentiert, so dass die Muss-Liste eine entsprechende Versionshistorie erhalten wird.

Wichtiger Hinweis:
Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, im Wege einer Vorabprüfung einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen aufweist und damit die Voraussetzungen des Art. 35 Abs. 1 Satz 1 DS-GVO erfüllt. Zum Begriff des Risikos wird auf die Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248 Rev. 01 17/DE angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017) der Art. 29 Datenschutzgruppe und das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen" der DSK verwiesen.

C Liste nach Art. 35 Abs. 4 DS-GVO

Maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen sind in der Leitlinie in WP 248 der Art. 29 Gruppe ab Seite 10 ff. wie folgt zu entnehmen:

1. **Bewerten oder Einstufen** (Scoring)
   ("Evaluation or scoring")
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
   ("Automated-decision making with legal or similar significant effect")
3. **Systematische Überwachung**
   ("Systematic monitoring")
4. **Vertrauliche oder höchst persönliche Daten**
   ("Sensitive data or data of a highly personal nature")
5. **Datenverarbeitung in großem Umfang**
   ("Data processed on a large scale")
6. **Abgleichen oder Zusammenführen von Datensätzen**
   ("Matching or combining datasets")
7. **Daten zu schutzbedürftigen Betroffenen**
   ("Data concerning vulnerable data subjects")
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
   ("Innovative use or applying new technological or organisational solutions")
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**
   ("When the processing in itself prevents data subjects from exercising a right or using a service or a contract")

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es jedoch auch vorkommen, dass nur eines der genannten Kriterien erfüllt wird und dennoch auf Grund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig wird.

Das Ergebnis der Vorabprüfung und die zugrunde gelegten Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.

Die folgende Liste wurde von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2018 beschlossen. Die englische Fassung der folgenden Liste ist ebenfalls veröffentlicht.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.
2	Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, , wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Früherkennung von Erbkrankheiten Genetische Datenbanken zur Abstammungsforschung	Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein. Ein Unternehmen bietet einen Dienst an, über den Kunden die eigenen genetischen Daten mit denen Dritter abgleichen können, um mehr über die eigene Abstammung zu erfahren. Dazu pflegt das Unternehmen eine Datenbank mit genetischen Daten einer Vielzahl von Personen.
3	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt	Betrieb eines Insolvenzverzeichnisses Träger von großen sozialen Einrichtungen Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an. Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut.
4	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
		Bilderzeugnisse von Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
		Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.	Ein Unternehmen verarbeitet die GPS-, Bluetooth- und/oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
		Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	
5	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können	Fraud-Prevention-Systeme	Zur Prävention von Betrugsfällen verarbeitet der Betreiber eines Online-Shops umfassende Datenmengen. Das Ergebnis der Prüfung ist ein Risikowert, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht.
		Scoring durch Auskunfteien, Banken oder Versicherungen	Eine Auskunftei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch. Eine Bank führt Scoring durch, um das Ausfallrisiko der Rückzahlungen von Personen zu bestimmen. Eine Versicherung führt ein Scoring durch, um das Risiko einer Person im Hinblick auf bestimmte Eigenschaften oder Aktivitäten der Person zur Bestimmung der Höhe einer Versicherungspolice zu bestimmen.
6	Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden.	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
7	Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	Betrieb von Bewertungsportalen	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Selbstständige oder Lehrer.
		Inkassodienstleistungen – Forderungsmanagement	Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen. Ggf. werden Daten an Auskunfteien übermittelt.
		Inkassodienstleistungen – Factoring	Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
			Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.
8	Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung der Aktivitäten (z.B. Internetverkehr, Mailverkehr und die Nutzung von Wechselmedien) am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
9	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	Betrieb von Dating- und Kontaktportalen Betrieb von großen Sozialen Netzwerken	Ein Webportal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
10	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	Eine Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
11	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	Kundensupport mittels künstlicher Intelligenz	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus. Ein Unternehmen setzt ein System ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet werden
12	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.	Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
		Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	
13	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
14	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Unternehmen verwendet Kundenkarten, welche das Einkaufsverhalten der Kunden erfassen. Als Anreiz zur Verwendung der Kundenkarte erhält der Kunde mit jedem Einkauf Treuepunkte. Mithilfe der gewonnenen Daten erstellt der Anbieter umfassende Kundenprofile.
15	Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte	Anonymisierung von besonderen Arten personenbezogener Daten nach Artikel 9	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,…) detailliert und systematisch zu erheben und zu verarbeiten.
17	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen.	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Ein Unternehmen bietet einen Dienst an, mit dem Daten aus Fitnessarmbändern zur Verbesserung des Trainings verarbeitet werden.

Hinweise

1. Diese Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Artikels 35 DSGVO enthaltenen allgemeinen Regelungen.
   Allgemein gilt, dass für jede Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Datenschutz-Folgenabschätzung durchgeführt werden muss, insbesondere in den in Absatz 3 genannten Fällen.

2. Diese Liste orientiert sich an der allgemeinen, im Arbeitspapier 248 Rev. 1 *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“* beschriebenen Vorgehensweise. Sie ergänzt und konkretisiert diese allgemeine Vorgehensweise.

Der Leitlinie sind folgende neun maßgebliche Kriterien aus WP 248 Rev. 01 zur Einordnung von Verarbeitungsvorgängen zu entnehmen:
a) Vertrauliche oder höchst persönliche Daten
b) Daten zu schutzbedürftigen Betroffenen
c) Datenverarbeitung in großem Umfang
d) Systematische Überwachung
e) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
f) Bewerten oder Einstufen (Scoring)
g) Abgleichen oder Zusammenführen von Datensätzen
h) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
i) Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

Version 1.1 vom 17.10.2018, ersetzt die Liste vom 18.07.2018

Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018

Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018

Der Kommissionsentwurf[1] zur ePrivacy-Verordnung vom Januar 2017 sieht vor, dass diese Verordnung, welche die ePrivacy-Richtlinie[2] ersetzen soll, gemeinsam mit der Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 in Kraft tritt und Geltung erlangt. Die ePrivacy-Verordnung soll die DSGVO im Hinblick auf die elektronische Kommunikation präzisieren und ergänzen.[3] Das Gesetzgebungsverfahren zur ePrivacy-Verordnung verzögert sich jedoch erheblich, so dass voraussichtlich nicht mehr mit einem Inkrafttreten im Jahr 2018 zu rechnen ist.[4]

Damit ergeben sich Fragen zur Anwendbarkeit nationalen Rechts neben der DSGVO. Der Gesetzgeber hat das Telemediengesetz (TMG) bisher nicht an die DSGVO angepasst, so dass die datenschutzrechtlichen Vorschriften des TMG (Abschnitt 4) voraussichtlich ab dem 25. Mai 2018 unverändert in Kraft sein werden.[5] Für die Rechtsanwender stellt sich wegen des Anwendungsvorrangs der DSGVO daher die Frage, ob die datenschutzrechtlichen Regelungen des TMG weiterhin anwendbar sein werden.

---

1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM/2017/010 final - 2017/03 (COD).

2 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 v. 31.07.2002, 37 und Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 337 v. 18.12.2009, 11.

3 ErwGr. 5 der ePrivacy-Verordnung(E), s. Fn. 1.

4 Insofern gilt nach dem 25. Mai 2018 die ePrivacy-Richtlinie weiter; S. dazu auch den Entwurf einer legislativen Entschließung des Europäischen Parlaments zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), worin im Gegensatz zum Kommissionsentwurf kein konkretes Datum zum Inkrafttreten mehr genannt ist.

5 S. zum Anpassungsbedarf aufgrund der Geltungserlangung der DSGVO: Gesetzentwurf der Fraktionen der CDU/CSU und SPD zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) mit Verweis auf eine Äußerung der Bundesregierung im Rechtsetzungsverfahren zum 2. TMG-Änderungsgesetz, BT-Drs. 18/12356 v. 16.05.2017, S. 28.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vertritt hierzu folgende Position:

1. Im Verhältnis zum nationalen Recht kommt ab dem 25. Mai 2018 die DSGVO für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung, es sei denn nationale Vorschriften sind aufgrund einer Kollisionsregel, eines Umsetzungsauftrages oder einer Öffnungsklausel der DSGVO vorrangig anwendbar.

2. Die DSGVO enthält in Artikel 95 eine Kollisionsregel zum Verhältnis der DSGVO zur ePrivacy-Richtlinie, wonach natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt werden, soweit sie besonderen in der ePrivacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

3. Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG. Denn diese Vorschriften stellen vorrangig eine Umsetzung der durch die DSGVO aufgehobenen Datenschutzrichtlinie[6] dar und unterfallen – da sie auch nicht auf der Grundlage von Öffnungsklauseln in der DSGVO beibehalten werden dürfen – demgemäß dem Anwendungsvorrang der DSGVO. Hiervon betroffen sind damit auch etwaige unvollständige Umsetzungen der ePrivacy-Richtlinie in diesem Abschnitt, welche jedenfalls isoliert nicht mehr bestehen bleiben können.

4. Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden.

[6] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.95, 31.

5. Eine unmittelbare Anwendung der ePrivacy-Richtlinie für die unter Ziffer 4 genannten Verarbeitungsvorgänge kommt nicht in Betracht (keine horizontale unmittelbare Wirkung von Richtlinien).

6. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kommt folglich nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DSGVO in Betracht. Darüber hinaus sind die allgemeinen Grundsätze aus Artikel 5 Absatz 1 DSGVO, sowie die besonderen Vorgaben z. B. aus Artikel 25 Absatz 2 DSGVO einzuhalten.

7. Verarbeitungen, die unbedingt erforderlich sind, damit der Anbieter den von den betroffenen Personen angefragten Dienst zur Verfügung stellen kann, können ggf. auf Art. 6 Absatz 1 Buchstabe b) oder Buchstabe f) DSGVO gestützt werden.[7]

8. Ob und inwieweit weitere Verarbeitungstätigkeiten rechtmäßig sind, muss durch eine Interessenabwägung im Einzelfall auf Grundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO geprüft werden.

9. Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO[8], in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

[7] S. zur Frage der Erforderlichkeit und zum dafür maßgeblichen Merkmal der Funktion *Artikel-29-Datenschutzgruppe*, WP 194 - Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht v. 07.06.2012, die in der englischen Version noch deutlicher herausstellt, dass es darauf ankommt, ob eine Verarbeitung für die „Auslieferung“ [delivery] des explizit nachgefragten Dienstes erforderlich ist, S. 3.

[8] S. zur Einwilligung *Artikel-29-Datenschutzgruppe*, WP 259 - Guidelines on Consent under Regulation 2016/679 v. 28.11.2017.

Diese Auffassung steht im Einklang mit dem europäischen Rechtsverständnis zu Artikel 5 Absatz 3 der ePrivacy-Richtlinie.[9] Im überwiegenden Teil der EU-Mitgliedsstaaten wurde die ePrivacy-Richtlinie vollständig in nationales Recht umgesetzt[10] oder die Aufsichtsbehörden fordern schon heute ein „Opt-in“ entsprechend Artikel 5 Absatz 3 der Richtlinie. Da die Verweise in der ePrivacy-Richtlinie auf die Datenschutzrichtlinie gemäß Artikel 94 Absatz 2 DSGVO als Verweise auf die DSGVO gelten, muss eine Einwilligung i. S. d. ePrivacy-Richtlinie europaweit ab dem 25.05.2018 den Anforderungen an eine Einwilligung nach der DSGVO genügen. Um in Zukunft einen einheitlichen Vollzug europäischen Datenschutzrechts zu gewährleisten, muss sichergestellt werden, dass auch Verantwortliche in Deutschland diese datenschutzrechtlichen Anforderungen umsetzen.

Dieses Papier wird unter Berücksichtigung der Entwicklungen auf europäischer Ebene fortgeschrieben.

[9] *Artikel-29-Datenschutzgruppe*, WP 194 - Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht v. 07.06.2012.

[10] *European Commission, Directorate-General of Communications Networks, Content & Technology*, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation v. 31.01.2015, Contract number: 30-CE-0629642/00-85, SMART 2013/0071, doi: 10.2759/411362.

Kurzpapier Nr. 10
Informationspflichten bei Dritt- und Direkterhebung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Bedeutung der Informationspflichten

Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmevorschriften greifen.

Die DS-GVO regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei der betroffenen Person (**Direkterhebung**, Art. 13 DS-GVO) oder bei Dritten (**Dritterhebung**, Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Information verantwortlich ist. Auch der Verantwortliche, der die Daten direkt bei der betroffenen Person erhoben hat, kann über Art. 13 DS-GVO hinaus zur Mitteilung nach Art. 14 Abs. 3 lit. c DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem anderen Empfänger offenbaren möchte.

Informationspflichten bei Direkterhebung

Bei der Informationspflicht im Falle der **Direkterhebung** wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DGS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).

Mitzuteilen sind nach Abs. 1:

- Name (ggf. Firmenname gem. § 17 Abs. 1 HGB oder Vereinsname gem. § 57 BGB) und Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreter
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und zusätzlich die Rechtsgrundlage, auf der die Verarbeitung fußt
- das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht (Art. 6 Abs. 1 lit. f DS-GVO)
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (vgl. Art. 4 Nr. 9 DS-GVO)
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und zugleich Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind)

Zusätzlich sind nach Abs. 2 Informationen über

- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkungs- und Wider-

spruchsrechte sowie das Recht auf Datenübertragbarkeit),

- das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt,
- das Beschwerderecht bei einer Aufsichtsbehörde,
- ggf. die gesetzliche oder vertragliche Verpflichtung des Verantwortlichen, personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich Profiling) aussagekräftige Informationen über die verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung

zur Verfügung zu stellen.

Informationspflichten bei Dritterhebung

Auch im Falle einer **Dritterhebung** unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Art. 14 Abs. 2 DS-GVO).

Art und Inhalt der mitzuteilenden bzw. der zur Verfügung zu stellenden Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitgeteilt werden müssen.

Allerdings hat die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt und somit auch keine Kenntnis darüber, welche personenbezogene Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 lit. d DS-GVO verpflichtet, die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für den Betroffenen erkennbar wird, zu welchen Folgen die Verarbeitung führen kann. Nur dann kann er eine bewusste Entscheidung darüber treffen, ob er ergänzend von seinem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch machen sollte.

Bei der Dritterhebung ist zudem nach Art. 14 Abs. 2 lit. f DS-GVO die Datenquelle anzugeben und, ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig festgestellt werden, muss dennoch eine allgemeine Information gegeben werden.

Bei der Dritterhebung ist weiterhin zu beachten, dass Angaben über die berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DS-GVO) nicht – wie bei der Direkterhebung – unter Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 lit. b DS-GVO).

Zweckänderung und Übermittlung

Die Informationspflichten im Falle einer Zweckänderung gelten sowohl für die Direkterhebung als auch für die Dritterhebung. Neben der Information über die geänderte Zweckbestimmung sind alle Informationspflichten gemäß Art. 13 Abs. 2 DS-GVO (Direkterhebung) oder gemäß Art. 14 Abs. 2 DS-GVO (Dritterhebung) erneut zu erfüllen.

Die Übermittlung an einen Dritten ist häufig eine Zweckänderung, so dass schon aus diesem Grund vor der Übermittlung die betroffene Person entsprechend zu informieren ist. Darüber hinaus stellt Art. 14 Abs. 3 lit. c DS-GVO klar, dass bei der Offenlegung an einen neuen Empfänger (einschließlich Auftragsverarbeitern, vgl. Art. 4 Nr. 9 DS-GVO) informiert werden muss, soweit dieser nicht von der bereits nach Artikel 13 Abs. 1 lit. e DS-GVO erteilten Information über Empfänger oder Empfängerkategorien umfasst ist.

Zeitpunkt der Erfüllung der Informationspflichten

Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.

Im Falle der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den spezifischen Umständen, darf aber einen Monat nicht überschreiten. Die Monatsfrist ist eine Maximaldauer und sollte nicht pauschal angesetzt werden. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.

Ausnahmen

Die Informationspflichten nach den Art. 13 und 14 DS-GVO bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Im Falle der Dritterhebung bestehen darüber hinaus keine Informationspflichten, wenn die Informationserteilung sich z. B. als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.

Außerdem sind in den §§ 32 und 33 des neuen Bundesdatenschutzgesetzes (BDSG-neu) weitere Ausnahmen von den Informationspflichten normiert. Die Informationspflicht nach Art. 13 DS-GVO soll beispielsweise gem. § 32 Abs. 1 Nr. 4 BDSG-neu nicht bestehen, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Es bestehen jedoch Zweifel, ob die in den §§ 32 und 33 BDSG-neu vorgesehenen Beschränkungen der Informationspflichten nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in den §§ 32 und 33 BDSG-neu vorgesehene Beschränkung der Informationspflichten aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Form der Informationspflicht

Gemäß Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen. Wird aber auf eine elektronisch verfügbare Information Bezug genommen, dann muss diese leicht auffindbar sein. Hierbei können auch Bildsymbole hilfreich sein.

Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. Dies gilt gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg.

Nachweise der Informationspflichten

Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 lit. a und Abs. 2 DS-GVO).

Folgen eines Verstoßes

Der Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 5 lit. b DS-GVO mit einer Geldbuße bestraft werden.

Empfehlung

Es ist für Verantwortliche im eigenen Interesse ratsam, rechtzeitig die nach Art. 25 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

17/EN

WP260 rev.01

Article 29 Working Party

Guidelines on transparency under Regulation 2016/679

Adopted on 29 November 2017

As last Revised and Adopted on 11 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of Contents

Introduction

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation[1] (the "**GDPR**"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights[2]. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680[3], these guidelines also apply to the interpretation of that principle.[4] These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

2. Transparency is a long established feature of the law of the EU[5]. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[2] These guidelines set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[4] While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be "lawful, fair and transparent" in relation to the natural persons concerned.

[5] Article 1 of the TEU refers to decisions being taken "*as openly as possible and as close to the citizen as possible*"; Article 11(2) states that "*The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society";* and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.

processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a)[6]), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles.[7] Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.[8] Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[9].

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/ notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights[10]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects.

---

[6] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

[7] In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).

[8] Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.

[9] The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.

[10] See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-201/14) at paragraph 74: *"the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".*

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.

The meaning of transparency

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:

> *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"*

Elements of transparency under the GDPR

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13 - 14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
- clear and plain language must be used (Article 12.1);
- the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
- it must be in writing *"or by other means, including where appropriate, by electronic means"* (Article 12.1);
- where requested by the data subject it may be provided orally (Article 12.1) ; and

- it generally must be provided free of charge (Article 12.5).

"*Concise, transparent, intelligible and easily accessible"*

8. The requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.

9. The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that *"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data…"* In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important *consequences* of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.

11. The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

Example

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.

"*Clear and plain language*"

12. With *written* information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed.[11] A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator[12] and is also explicitly referred to in the context of consent in Recital 42 of the GDPR[13]. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different

[11] See How to Write Clearly by the European Commission (2011), to be found at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

[13] Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.

interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

Poor Practice Examples

The following phrases are not sufficiently clear as to the purposes of processing:

- "*We may use your personal data to develop new services"* (as it is unclear what the "services" are or how the data will help develop them);
- "*We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and
- "*We may use your personal data to offer personalised services"* (as it is unclear what the "personalisation" entails).

Good Practice Examples[14]

- *"We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in "* (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
- *"We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive"* (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
- "*We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read"* (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical

[14] The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.

relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets[15] data subjects speaking those languages.)

Providing information to children and other vulnerable people

14. Where a data controller is targeting children[16] or is, or should be, aware that their goods/ services are particularly utilised by children (including where the controller is relying on the consent of the child)[17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them.[18] A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".[19]

15. WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds.[20] It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age,[21] Article 8 *does not provide* for transparency measures to be directed at the holder of parental responsibility who

[15] For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.

[16] The term "child" is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years.

[17] i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).

[18] Recital 38 states that "Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". Recital 58 states that "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand".

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

[20] Article 13 of the UN Convention on the Rights of the Child states that: "The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."

[21] See footnote 17 above.

gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.

16. Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.[22] This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.

"In writing or by other means"

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing.[23] (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified "means" including electronic means to be used. WP29's position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37).[24] However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of *methods* to ensure transparency in relation to processing.

[22] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.

[23] Article 12.1 refers to "language" and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

[24] The WP29's recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.

18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used *in addition* to a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts.[25] "Other means", which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject's information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative *additional* means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things[26] (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

"*..the information may be provided orally"*

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are a specific named person and the means should enable the controller to verify a data subject's identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to *future* users/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under

[25] These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.

[26] WP29 Opinion 8/2014 adopted on 16 September 2014

Articles 13 and 14 may be provided by oral means without the controller requiring a data subject's identity to be proven.

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject's identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

"Free of charge"

22. Under Article 12.5,[27] data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects).[28] This aspect of transparency also means that any information provided under the transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods.[29]

Information to be provided to the data subject – Articles 13 & 14

Content

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The **table in the Annex** to these

[27] This states that "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."

[28] However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).

[29] By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained".

guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.

"Appropriate measures"

24. As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller's responsibility to take "appropriate measures" in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/ service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.

25. In order to help identify the most appropriate modality for providing the information, in advance of "going live", data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardised tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances.

Timing for provision of information

26. Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle[30]. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:

[30] Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.

- a data subject consciously provides to a data controller (e.g. when completing an online form); or
- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:

- third party data controllers;
- publicly available sources;
- data brokers; or
- other data subjects.

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided *"at the time when personal data are obtained".* In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:

- The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, *"having regard to the specific circumstances in which the personal data are processed"* (Article 14.3(a)).

- The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b),[31] which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided at the latest at the time of the first communication with the data subject. If the first communication occurs prior to the one-month time limit after obtaining the personal data, then the information must be provided *at the latest* at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

[31] The use of the words *"if the personal data are to be used for.."* in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.

- The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c)[32] which provides for a situation where the data are being disclosed to another recipient (whether a third party or not)[33]. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided *at the latest* at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

28. Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be *"made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing".* Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

Changes to Article 13 and Article 14 information

29. Being accountable as regards transparency applies not only at the point of collection of personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the

[32] The use of the words *"if a disclosure to anther recipient is envisaged…"* in Article 14.3(c) likewise indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.

[33] Article 4.9 defines "recipient" and clarifies that a recipient to whom personal data are disclosed does not have to be a third party. Therefore, a recipient may be a data controller, joint controller or processor.

change would be to data subjects. Changes to a privacy statement/ notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation to the processing. Conversely, an example of changes to a privacy statement/ notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/ grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/ notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(a). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

Timing of notification of changes to Article 13 and Article 14 information

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 45). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the

change taking effect satisfies the principle of fairness to the data subject. Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.

32. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/ notice and where they can find it.

Modalities - format of information provision

33. Both Articles 13 and 14 refer to the obligation on the data controller to *"provide the data subject with all of the following information…"* The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.

Layered approach in a digital environment and layered privacy statements/ notices

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39.[34] While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use *additional* transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the

[34] Recital 39 states, on the principle of transparency, that "That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."

use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

Layered approach in a non-digital environment

38. A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.

"Push" and "pull" notices

39. Another possible way of providing transparency information is through the use of "push" and "pull" notices. Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, privacy dashboards and "learn more" tutorials. These allow for a more user-centric transparency experience for the data subject.

- A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of

demonstrating that 'privacy information' is a necessary and integral part of a service rather than a lengthy list of legalese.

- A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.

Other types of "appropriate measures"

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29's position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/ online presence, is to do so through an electronic privacy statement/ notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence) use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

a. Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;
b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;
c. Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;
d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;

e. "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.

Information on profiling and automated decision-making

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling[35] which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(f) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal data, equally apply to profiling generally (not just profiling which is captured by Article 22[36]), as a type of processing.[37]

Other issues – risks, rules and safeguards

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs,[38] data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

[36] This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.

[37] Recital 60, which is relevant here, states that "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".

[38] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.1

protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data controllers must be made available to the data subject. In other words, it must be completely clear to a data a subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR.[39]

Information related to further processing

45. Both Articles 13 and Article 14 contain a provision[40] that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/ obtained. If so, "*the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2".* These provisions specifically give effect to the principle in Article 5.1(b) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is *incompatible* with these purposes is prohibited.[41] The second part of Article 5.1(b) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are *compatible* with the original purposes (Article 6.4 informs this issue[42]), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing

[39] Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

[40] At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word "collected", which is used in Article 13, and which is replaced with the word "obtained" in Article 14.

[41] See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89

[42] Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.

for a particular purpose may take place.[43] In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

46. Articles 13.3 and 14.4, insofar as they refer to the provision of "*any relevant further information as referred to in paragraph 2",* may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "*other necessary information*".) However the default position is that all such information set out in that sub-article should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice on the compatibility analysis carried out under Article 6.4[44] where a legal basis other than consent or national/ EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others.[45] Where controllers choose not to include such information in a privacy notice/ statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

48. Connected to the exercise of data subject rights is the issue of timing. As emphasised above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to *further processing* must be provided "prior to that further processing". WP29's position is that a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

[43] Recitals 47 and 50

[44] Also referenced in Recital 50

[45] As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and to verify the lawfulness of the processing.

Visualisation tools

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58[46] indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online environment.[47]

Icons

50. Recital 60 makes provision for information to be provided to a data subject "in combination" with standardised icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:

> "*The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable".*

51. As Article 12.7 states that "*Where the icons are presented electronically, they shall be machine-readable"*, this suggests that there may be situations where icons are not presented electronically,[48] for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardisation of symbols/ images to be

[46] "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."

[47] In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).

[48] There is no definition of "machine-readable" in the GDPR but Recital 21 of Directive 2013/37/EU17 defines "machine-readable" as:

"a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats."

universally used and recognised across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons.[49] WP29 recognises that, in line with Recital 166, the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.

Certification mechanisms, seals and marks

53. Aside from the use of standardised icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects.[50] WP29 will be issuing guidelines on certification mechanisms in due course.

Exercise of data subjects' rights

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned, as they must:[51]

- provide information to data subjects on their rights[52] (as required under Articles 13.2(b) and 14.2(c));
- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and
- facilitate the exercise of data subjects' rights under Articles 15 to 22.

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to *meaningfully position* data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data. Recital 59 emphasises that *"modalities should be provided for facilitating the exercise of the data subject's rights"* and that the data controller should *"also provide means*

[49] Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

[50] See the reference in Recital 100

[51] Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)

[52] Access, rectification, erasure, restriction on processing, object to processing, portability

for requests to be made electronically, especially where personal data are processed by electronic means". The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

Example

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.

Exceptions to the obligation to provide information

Article 13 exceptions

56. The only exception to a data controller's Article 13 obligations where it has collected personal data directly from a data subject occurs *"where and insofar as, the data subject already has the information".*[53] The principle of accountability requires that data controllers demonstrate (and document) what information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase "insofar as" in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

Example

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already

[53] Article 13.4

has from 6 months ago and which has not since changed (e.g. the identity and contact details of the controller and the data protection officer, information on data subject rights and the right to complain to the relevant supervisory authority). As a matter of best practice however, the complete suite of information should be provided to the data subject again but the data subject also should be able to easily tell what information amongst it is new. The new processing for the purposes of the instant messaging service may affect the data subject in a way which would prompt them to seek to exercise a right they may have forgotten about, having been informed six months prior. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and their rights.

Article 14 exceptions

57. Article 14 carves out a much broader set of exceptions to the information obligation on a data controller where personal data has not been obtained from the data subject. These exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the circumstances where the data subject already has the information in question (Article 14.5(a)), Article 14.5 also allows for the following exceptions:

- The provision of such information is impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or where it would make the achievement of the objectives of the processing impossible or seriously impair them;
- The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests ; or
- An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential.

Proves impossible, disproportionate effort and serious impairment of objectives

58. Article 14.5(b) allows for 3 separate situations where the obligation to provide the information set out in Articles 14.1, 14.2 and 14.4 is lifted:

(i) Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/ historical research or statistical purposes); or
(iii) Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.

"Proves impossible"

59. The situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually *prevent it* from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.

Example

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller's protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject's address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.

Impossibility of providing the source of the data

60. Recital 61 states that "*where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided*". The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default,[54] transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).

[54] Article 25

"Disproportionate effort"

61. Under Article 14.5(b), as with the "proves impossible" situation, "disproportionate effort" may also apply, in particular, for processing *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)".* Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29's position is that this exception should not be *routinely* relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(b), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.

> **Example**
>
> A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14 information.

> **Example**
>
> Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50

years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

64. Where a data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(b) specifies that the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(b), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimising the data collected and the storage period; and implementing technical and organisational measures to ensure a high level of security. Furthermore, there may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

Serious impairment of objectives

65. The final situation covered by Article 14.5(b) is where a data controller's provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(b) pre-supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis.

Example

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in

another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to "tip off" the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(b) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder's personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of "tip-offs". However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

Obtaining or disclosing is expressly laid down in law

66. Article 14.5(c) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data *"is expressly laid down by Union or Member State law to which the controller is subject".* This exemption is conditional upon the law in question providing *"appropriate measures to protect the data subject's legitimate interests".* Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides "*appropriate measures to protect the data subject's legitimate interests",* the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data *directly from a data subject*, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.

Example

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained

from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.

Confidentiality by virtue of a secrecy obligation

67. Article 14.5(d) provides for an exemption to the information requirement upon data controllers where the personal data *"must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy".* Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

Example

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(d) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

Restrictions on data subject rights

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights[55] where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on

[55] As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.

their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such *a national legislative restriction* to the exercise of data subject rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/ 2017[56] that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.

Transparency and data breaches

70. WP29 has produced separate Guidelines on Data Breaches[57] but for the purposes of these guidelines, a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12.[58] The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

[56] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2

[57] Guidelines on Personal data breach notification under Regulation 2016/679, WP 250

[58] This is made clear by Article 12.1 which specifically refers to "…any communication under Articles 15 to 22 **and 34** relating to processing to the data subject…" [emphasis added].

Annex
Information that must be provided to a data subject under Article 13 or Article 14

Required Information Type	Relevant article (if personal data collected directly from data subject)	Relevant article (if personal data not obtained from the data subject)	WP29 comments on information requirement
The identity and contact details of the controller and, where applicable, their representative[59]	Article 13.1(a)	Article 14.1(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc.)
Contact details for the data protection officer, where applicable	Article 13.1(b)	Article 14.1(b)	See WP29 Guidelines on Data Protection Officers[60]
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.1(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security

[59] As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means a natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the EU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behaviour of, data subjects in the EU.

[60] Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017

			measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.
Where legitimate interests (Article 6.1(f)) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party	Article 13.1(d)	Article 14.2(b)	The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the *balancing test*, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. To avoid information fatigue, this can be included within a layered privacy statement/ notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.
Categories of personal data concerned	Not required	Article 14.1(d)	This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained.

Recipients[61] (or categories of recipients) of the personal data	Article 13.1(e)	Article 14.1(e)	The term "recipient" is defined in Article 4.9 as "*a natural or legal person, public authority, agency or another body, to which the personal data are disclosed,* ***whether a third party or not****" [emphasis added].* As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.
Details of transfers to third countries, the fact of same and the details of the relevant	Article 13.1(f)	Article 14.1(f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article

[61] As defined by Article 4.9 of the GDPR and referenced in Recital 31

safeguards[62] (including the existence or absence of a Commission adequacy decision[63]) and the means to obtain a copy of them or where they have been made available			45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.
The storage period (or if not possible, criteria used to determine that period)	Article 13.2(a)	Article 14.2(a)	This is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different

[62] As set out in Article 46.2 and 46.3

[63] In accordance with Article 45

			categories of personal data and/or different processing purposes, including where appropriate, archiving periods.
The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing and • portability.	Article 13.2(b)	Article 14.2(c)	This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.[64] In relation to the right to portability, see WP29 Guidelines on the right to data portability.[65]
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	Article 13.2(c)	Article 14.2(d)	This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.[66]
The right to lodge a complaint with a supervisory authority	Article 13.2(d)	Article 14.2(e)	This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to	Article 13.2(e)	Not required	For example in an employment context, it may be a contractual requirement to provide certain

[64] Article 21.4 and Recital 70 (which applies in the case of direct marketing)

[65] Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017

[66] Article 7.3

enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.			information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields.
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source	Not required	Article 14.2(f)	The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/ privately held sources) and the types of organisation/ industry/ sector.
The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the data subject	Article 13.2(f)	Article 14.2(g)	See WP29 Guidelines on automated individual decision-making and Profiling.[67]

[67] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

---

[1] See Article 4(21) of the GDPR

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

[7] See Articles 34(4) and 58(2)(e)

Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.

I. Personal data breach notification under the GDPR

A. Basic security considerations

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

---

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).

[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] See Articles 5(1)(f) and 32.

[11] Article 32; see also Recital 83

[12] See Recital 87

B. What is a personal data breach?

1. Definition

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a "personal data breach" in Article 4(12) as:

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Example

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].

The potential adverse effects of a breach on individuals are considered below.

2. Types of personal data breaches

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access[15] to, or destruction of, personal data.

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

[14] See Opinion 03/2014

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information,"

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12).

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

Examples

available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: " Timely, reliable access to data and information services for authorized users." See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] See Article 33(5)

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

3. The possible consequences of a personal data breach

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[17].

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is

[17] See also Recitals 85 and 75

[18] See also Recital 86.

presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state: "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

II. Article 33 - Notification to the supervisory authority

A. When to notify

1. Article 33 requirements

Article 33(1) provides that:

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Recital 87 states[20]:

> "It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

2. When does a controller become "aware"?

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Recital 85 is also important here.

controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact

[21] See Recital 87

assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

Example

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach.
- Documentation of the breach should take place as it develops.

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

3. Joint controllers

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

4. Processor obligations

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends the

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] See also Recital 79.

processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.

B. Providing information to the supervisory authority

1. Information to be provided

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:

> "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

Article 33(3) states that the controller "shall at least" provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

Example

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

In any event, the supervisory authority may request further details as part of its investigation into a breach.

2. Notification in phases

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states:

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the

[26] See Article 9.

breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

Example

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

3. Delayed notifications

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

C. Cross-border breaches and breaches at non-EU establishments

1. Cross-border breaches

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that:

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."

However, Article 56(1) states:

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

Furthermore, Article 56(6) states:

> "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

2. Breaches at non-EU establishments

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]:

---

[27] See Article 4(23)

[28] See also Recital 122.

[29] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] See also Recitals 23 and 24

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Article 3(3) is also relevant and states[32]:

"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).

D. Conditions where notification is not required

Article 33(1) makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

[32] See also Recital 25

[33] See Recital 80 and Article 27

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] See also Article 4(1) and (2) of Regulation 611/2013.

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Example

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

III. **Article 34 – Communication to the data subject**

A. Informing individuals

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) states:

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

B. Information to be provided

When notifying individuals, Article 34(2) specifies that:

> "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."

According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

[36] See also Recital 86.

C. Contacting individuals

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

At the same time, Recital 86 explains that:

> "Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

D. Conditions where communication is not required

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

IV. Assessing risk and high risk

A. Risk as a trigger for notification

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] See Article 5(2)

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

B. Factors to consider when assessing risk

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

[39] See Recital 75 and Recital 85.

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]:

- The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- The nature, sensitivity, and volume of personal data

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- Ease of identification of individuals

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- Severity of consequences for individuals.

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal

data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].

V. Accountability and record keeping

A. Documenting breaches

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains:

> "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with Article 83.

B. Role of the Data Protection Officer

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

---

[44] See Article 5

[45] See Article 6 and also Article 9.

[46] See Article 5(1)(e).

[47] See Recital 85

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

VI. Notification obligations under other legal instruments

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

51 Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*

GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).

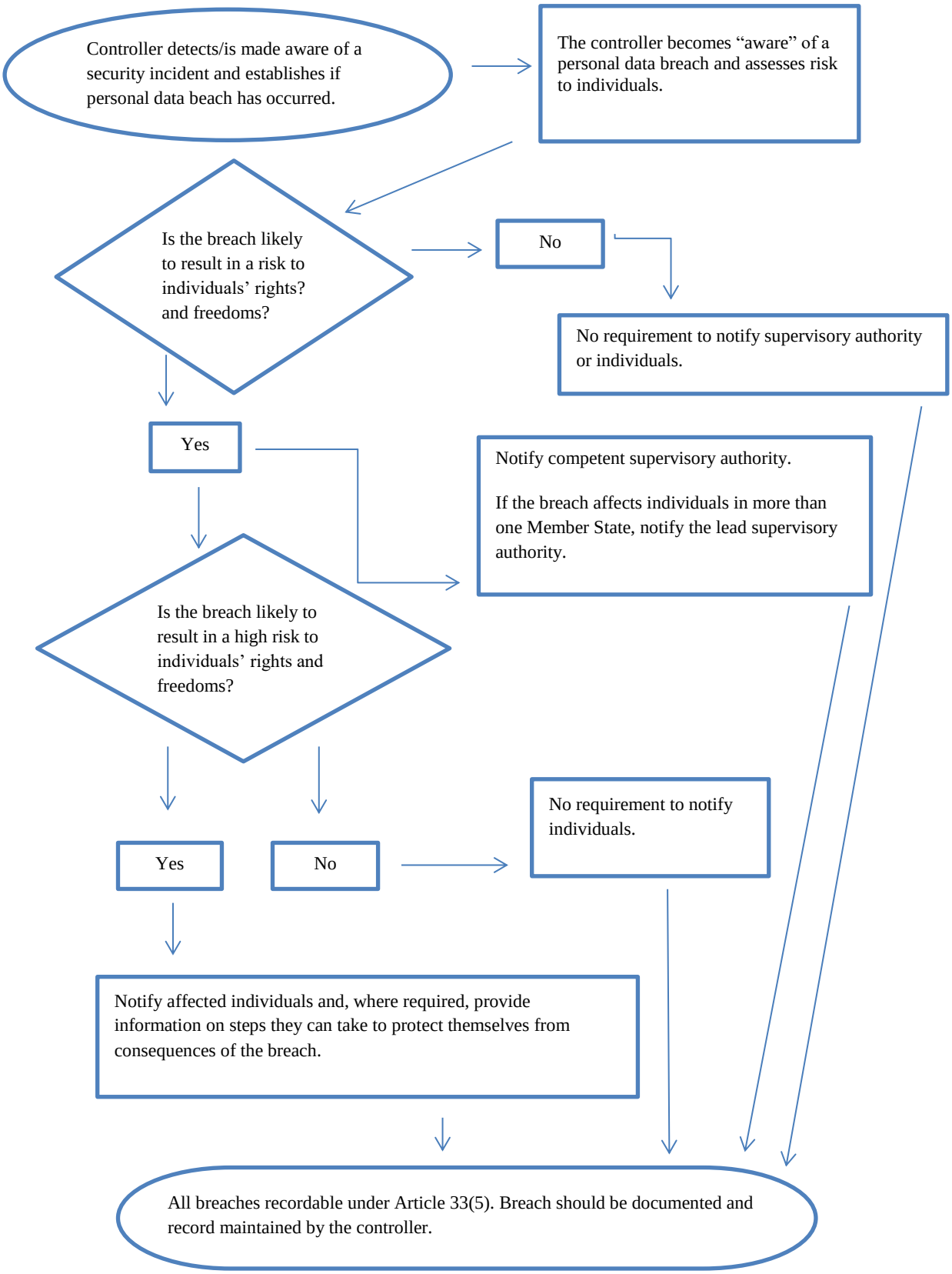
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52] must notify breaches to the competent national authorities.

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Annex**

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	**Notify the supervisory authority?**	**Notify the data subject?**	**Notes/recommendations**
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

functionality was to encrypt the data, and that there was no other malware present in the system.		consequences.	confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which	As the processor, the website hosting company must notify its affected clients (the controllers) without	If there is likely no high risk to the individuals they do not need to be	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS

controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	notified.	Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Vermerk:

Rechtliche Bewertung von Fotografien einer unüberschaubaren Anzahl von Menschen nach der DSGVO außerhalb des Journalismus

I. Frage und Problemstellung

Wie sind Bildaufnahmen, die nicht im journalistischen Umfeld oder zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten von einer großen Anzahl von Personen, insbesondere im öffentlichen Raum angefertigt werden ab Inkrafttreten der DSGVO zu bewerten?

Die Problematik stellt sich dabei wie folgt dar: Auf der einen Seite liegen bei Bildaufnahmen nahezu immer personenbeziehbare Daten vor, die dem Verbot mit Erlaubnisvorbehalt der DSGVO unterfallen. Auf der anderen Seite ist es nicht möglich, bei Aufnahmen, auf denen viele Personen zu sehen sind, diese tatsächlich zu identifizieren oder diese zu kontaktieren. Daher ist die Einholung einer Einwilligung oder die Information der Abgelichteten über Ihre Rechte für die Fotografen nahezu unmöglich.
Besteht also entweder ein Einwilligungserfordernis oder eine Informationspflicht aller Abgebildeten, so wären etwa Bildaufnahmen von Wahrzeichen, Sehenswürdigkeiten, oder Sportereignissen, bei denen meist viele Menschen zu sehen sind, nach der DSGVO nicht mehr rechtskonform möglich. Zu untersuchen ist daher, ob Aufnahmen nach der DSGVO gerechtfertigt werden können (II.) und ob eine Informationspflicht gegenüber den Abgebildeten (III.) besteht.

II. Rechtmäßigkeit der Aufnahmen

Einleitend ist festzuhalten, dass Aufnahmen, die zu rein privaten Zwecken gemacht werden, nicht dem Anwendungsbereich der DSGVO unterfallen, wie sich aus Art. 2 Abs. 1 lit. c DSGVO ergibt. Problematisch sind vielmehr solche Aufnahmen, die zu kommerziellen oder künstlerischen Zwecken gefertigt werden und nicht Art. 2 Abs. 1 lit. c DSGVO unterfallen.

In der heutigen Zeit wird man angesichts der weit überwiegend digitalen Fotografie von einer automatisierten Datenverarbeitung und damit von der Anwendbarkeit der DSGVO auszugehen haben.

Nach Art. 6 Abs. 1 DSGVO ist eine Verarbeitung personenbezogener Daten rechtfertigungsbedürftig. Personenbezogene Daten liegen dabei gemäß Art. 4 Ziff. 1 DSGVO vor, wenn sie sich auf „eine identifizierbare natürliche Person beziehen“. Identifizierbar ist eine Person, wenn diese „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“.

Fotografien von Betroffenen, die heute fast ausschließlich mit Digitalkameras aufgenommen werden, stellen grundsätzlich personenbezogene Daten dar. Es handelt sich um physische und physiologische Merkmale, die auch sofort, mit den entsprechenden Metadaten, digital gespeichert werden. Die Metadaten umfassen dabei zumindest Ort und Zeit des Bildes. Auch wird häufig der Standort gespeichert. In jedem Fall lässt sich der Standort anhand der Aufnahme ermitteln. Weiterhin lassen sich Gesichter mit entsprechenden Datenbanken abgleichen und sich so weitere Daten ermitteln, wie z.B. die Namen der Betroffenen. An der prinzipiellen Identifizierbarkeit ändert auch der Umstand nichts, dass der einzelne Fotograf

in den meisten Fällen keine Zuordnung einzelner Gesichter zu anderen Daten dieser Personen herstellt oder überhaupt selbst herstellen kann. Auf die individuellen Möglichkeiten des einzelnen Fotografen ist bei abstrakter Betrachtung, ob es sich um personenbezogene Daten handelt, nicht abzustellen.[1] Es reicht aus, dass eine Personenbeziehbarkeit der Daten prinzipiell möglich ist, was angesichts der hohen Auflösung von Digitalbildern in Bezug auf Bildaufnahmen und der Verfügbarkeit von Gesichtserkennungssoftware angenommen werden muss.[2] Auch wenn man auf die individuellen Fähigkeiten des einzelnen Fotografen abstellen würde, also einen relativen Begriff der personenbezogenen Daten vertritt, wird man wohl zugestehen müssen, dass die körperlichen Merkmale einer Person, insbesondere deren individuelle Gesichtszüge, wenn sie ausreichend erkennbar sind, immer geeignet sind eine Person eindeutig zu identifizieren. Es handelt sich daher bei ausreichend aufgelösten Bildaufnahmen, die eine Person gut erkennbar zeigen, immer um personenbezogene Daten.

Bildaufnahmen sind daher zunächst nach Art. 6 Abs. 1 DSGVO verboten, wenn sie nicht auf eine Einwilligung oder auf eine andere Rechtfertigung gestützt werden können.
Bei Bildaufnahmen von Menschenmengen können in der Regel keine Einwilligungen eingeholt werden und diese daher auch nicht auf den Rechtfertigungsgrund des Art. 6 Abs. 1 lit. a DSGVO gestützt werden. Dies wäre bei Bildaufnahmen von Wahrzeichen, Sehenswürdigkeiten sowie Sportereignissen für einen einzelnen Fotografen auch gar nicht durchführbar. Demnach bedarf es für die Datenerhebung einer anderen Rechtfertigung.

Eine solche Rechtfertigung kann hier nicht dem KUG entnommen werden. Unabhängig von der Frage der Anwendbarkeit des KUG neben der DSGVO[3] enthält das KUG schon keine

[1] a.A. Gola in: Gola, DS-GVO, § 2 Rn. 10.
[2] EuGH, Urt. vom 19.10.2016 – Rs. C-582/14 stellt insoweit auf die abstrakte Möglichkeit ab, dass der Verantwortliche sich der verfügbaren Identifizierungsmöglichkeiten bedienen kann. Vgl. auch Ziebarth in: Sydow, DS-GVO, Art. 4 Rn. 37.
[3] Vor dem Inkrafttreten der DSGVO war das KUG als lex specialis zum BDSG anzusehen, § 1 Abs. 3 Satz 1 BDSG. § 1 Abs. 2 Satz 1 BDSG-neu kommt aufgrund des Anwendungsvorranges der DSGVO keine vergleichbarer Regelungsgehalt zu.

Rechtsgrundlage für die Datenerhebung, sondern lediglich für die Veröffentlichung der Bilder.[4] Die Zulässigkeit der Ablichtung als Vorstadium der Veröffentlichung wurde nach der bisherigen Rechtslage an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gemessen bzw. in diesem Rahmen eine Interessenabwägung vorgenommen.[5] Da nunmehr eine spezielle Regelung für diese Abwägung in Form des Art. 6 DSGVO besteht, die zudem als europarechtliche Verordnung grundsätzlich auch gegenüber dem deutschen Verfassungsrecht Anwendungsvorrang genießt, ist die Rechtmäßigkeit der Ablichtung ausschließlich hiernach zu beurteilen.

Eine Rechtfertigung aufgrund eines einfachen Gesetzten wäre nach Art. 85 Abs. 2 DSGVO grundsätzlich möglich. Nach Art. 85 Abs. 2 DSGVO können die Mitgliedsstaaten für Verarbeitungen zu künstlerischen Zwecken Abweichungen oder Ausnahmen von Kapitel II, also auch von Art. 6 DSGVO, vorsehen. Ein solches Gesetz wäre auch wünschenswert. Eine einfachgesetzliche Regelung, die den künstlerischen Bereich regelt und dabei Anwendungsfälle wie den hier in Frage stehenden, grundsätzlich erlaubt, ohne dass die Rechtmäßigkeit erst durch eine Abwägung ermittelt werden muss, wäre dem Stellenwert der künstlerischen Betätigung in Deutschland angemessener. Dass der europäische Verordnungsgeber eine solche Ausgestaltung durch die Mitgliedsstaaten bei der Schaffung des Art. 85 DSGVO im Blick hatte, zeigt Erwägungsgrund 153 der diesbezüglich folgenden Auftrag für die Mitgliedstaaten formuliert: „für die Verarbeitung personenbezogener Daten ausschließlich zu […] künstlerischen […] Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten. […] Dies insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich.“ Eine solche Regelung auf Grundlage des Art. 85 Abs. 2 DSGVO hat der deutsche Gesetzgeber allerdings bislang nicht erlassen.

[4] Vgl §§ 22, 23 KUG.
[5] Götting in: Schricker/Löwenheim, Urheberrecht, § 22 KUG Rn. 35.

Die Aufnahmen der oben genannten Motive können, solange eine Regelung auf Grundlage der Öffnungsklausel des Art. 85 Abs. 2 DSGVO nicht vorliegt, im Regelfall wohl nach Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden. Es besteht ein berechtigtes Interesse der Fotografen daran, ihre Betätigung, die im Regelfall dem Kunstbegriff unterfällt, auszuüben. Die Kunstfreiheit wird durch Art. 13 GRCh geschützt. Nach Art. 52 Abs. 4 GRCh werden Grundrechte, die „sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, im Einklang mit diesen Überlieferungen ausgelegt". Daher kann auch an dieser Stelle die ausdifferenzierte Rechtsprechung zum Recht am eigenen Bild, die als mitgliedsstaatliche Verfassungstradition angesehen werden kann, mit einbezogen werden. In dieser wird die künstlerische Betätigung zumeist dem Recht am eigenen Bild in den hier geschilderten Fällen übergeordnet.[6]

Dem so festgestellten Interesse an der Freiheit der künstlerischen Betätigung werden im Regelfall keine schutzwürdigen Interessen der Betroffenen entgegenstehen, insbesondere da diese nur in ihrer Sozialsphäre betroffen sind. In Einzelfällen können sich schutzwürdige Interessen ergeben, die eine Einzelfallabwägung notwendig machen. Der BGH nimmt eine solche Abwägung anhand des Art. 5 Abs. 1 GG vor - bezogen auf die Rechtslage vor der DSGVO im Rahmen des § 29 Abs. 1 Nr. 1 BDSG. Demnach ist die Datenerhebung zulässig, wenn „[…]kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat[…]".[7] Die Interessenabwägung zwischen dem berechtigten Interesse des Verantwortlichen und den schutzwürdiges Interessen des Betroffenen ist insoweit vergleichbar mit der Abwägung bei Art. 6 Abs. 1 lit. f DSGVO.[8] Insbesondere bei der Ablichtung von Kindern ist Art. 6 Abs. Absatz 1 lit. f a.E. zu beachten.[9]

III. Informationspflichten gegenüber den Betroffenen

[6] Entsprechend der gesetzgeberischen Wertung des § 23 Abs. 1 (insb. Ziff. 2) KUG.
[7] BGH Urteil vom 23. September 2014 - VI ZR 358/13.
[8] BeckOK Datenschutzrecht/Alber Art. 6 DSGVO Rn. 48 sieht die Rechtsprechung zu § 28 ff. BDSG als Auslegungshilfe zu Art. 6 lit. f DSGVO an.
[9] BeckOK Datenschutzrecht/Alber Art. 6 DSGVO Rn. 51

Unabhängig von der Frage der Rechtmäßigkeit der Erhebung der Daten stellt sich weiterhin die Frage, ob und in welchem Maße die abgebildeten Personen entweder nach Art. 13 oder nach 14 DSGVO zu informieren sind. Die Informationspflichten nach der DSGVO sind dabei umfassend und grundsätzlich jedem Betroffenen zu erteilen. Eine Ausnahme von den Informationspflichten insgesamt enthält Art. 11 DSGVO. Dessen Voraussetzungen sind daher vorrangig zu prüfen.

Nach Art. 11 Abs. 1 DSGVO ist ein Verantwortlicher nicht verpflichtet, zur bloßen Einhaltung der DSGVO zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren, falls für die Zwecke, für die dieser die personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich ist. Dies ist nach dem oben bereits Gesagten zumeist der Fall. Der einzelne Fotograf hat im Regelfall weder ein Interesse daran, noch die Möglichkeit, die auf dem Bild abgebildeten Personen ohne erheblichen Aufwand zu identifizieren. Eine solche Identifizierung würde dann alleine aus dem Grund erfolgen, um die Vorgaben der Art. 13, 14 DSGVO zu erfüllen. Dies soll durch die Regelung des Art. 11 DSGVO gerade verhindert werden, da in einem solchen Fall die Information der Betroffenen keine Stärkung Ihrer Rechte, sondern eine Vertiefung des Eingriffs in ihr Persönlichkeitsrecht durch die Identifizierung bedeuten würde.[10]

Teilt man die Auffassung nicht, dass Art. 11 Abs. 1 DSGVO in diesen Fällen einschlägig ist, so muss die Frage beantwortet werden, ob eine Pflicht zur Information nach Art. 13 oder 14 DSGVO besteht. Bei einer Anwendung des Art. 13 DSGVO wären für die vorliegende Konstellation keine Ausnahmen von der Informationspflicht vorgesehen. Dies würde bedeuten, dass ein Fotograf alle auf einem entsprechenden Bild erkennbaren Personen gemäß Art. 13 DSGVO zu informieren hätte. Lediglich bei Anwendung des Art. 14 DSGVO

[10] So auch Klein, Personenbilder im Spannungsfeld zwischen DSGVO und KUG, S. 243.

besteht mit Art. 14 Abs. 5 DSGVO ein Ausnahmetatbestand, der eine Einzelfallbetrachtung ermöglicht.

Zunächst ist daher abzugrenzen, ob die Datenerhebung **bei** der betroffenen Person erfolgt. In diesem Fall richtet sich die Informationspflicht nach Art. 13 DSGVO. Anderenfalls nach Art. 14 DSGVO.

Entscheidend ist daher, wie der Passus „**bei** der betroffenen Person" auszulegen ist. Es wird vertreten, dass eine Erhebung beim Betroffenen dann anzunehmen ist, wenn die Person direkt als Quelle der Datenerhebung dient.[11] Eine Erhebung nicht bei der betroffenen Person liegt nach dieser Auffassung dann vor, wenn die Daten aus einer dritten Quelle stammen. Hierbei wird für eine Datenerhebung bei der betroffenen Person teilweise als ausreichend angesehen, dass es dem Verantwortlichen zum Zeitpunkt der Datenerhebung prinzipiell möglich ist, den Betroffenen zu kontaktieren und ihm die Informationen zur Verfügung zu stellen.[12] Bei den hier in Frage stehenden Konstellationen würde man zumeist zu dem Ergebnis kommen müssen, dass die Personen für den Fotografen grundsätzlich kontaktierbar sind, da sie in Reichweite seiner Kamera sind. Zu berücksichtigen ist dabei jedoch auch, dass die Reichweite der Kamera in etlichen Fällen die Reichweite des Fotografen selbst zwecks Kontaktaufnahme übersteigt.

Andererseits wird zur Abgrenzung darauf abgestellt, ob der Betroffene die Datenerhebung zur Kenntnis nimmt oder nehmen kann und daher auf den Vorgang der Datenerhebung Einfluss nehmen kann.[13] Dafür spricht, dass das Fotografieren, das eine größere Anzahl an Subjekten erfasst, mit der heimlichen Erhebung von Daten vergleichbar ist. Insbesondere mit Fällen der heimlichen Videoüberwachung. Art. 14 Abs. 5 lit. d DSGVO zeigt, dass die DSGVO davon ausgeht, dass Art. 14 DSGVO in Fällen der heimlichen Datenerhebung Anwendung findet.[14] Ansonsten wäre diese nie zulässig. Dass dies nicht gewollt ist, zeigt schon die Existenz des Art. 14 Abs. 5 lit. d DSGVO. Auch bezüglich der heimlichen Videoüberwachung

[11] Bäcker, in: Kühling/Buchner, DS-GVO, Art. 14 Rn. 9.
[12] So Bäcker, in: Kühling/Buchner, DS-GVO, Art. 13 Rn. 13.
[13] Franck in: Gola, DS-GVO, Art. 13 Rn. 4; i.E. Schmidt-Wudy in: BeckOK DatenschutzR/ DS-GVO, Art. 14 Rn. 31 sowie Albert Ingold in: Sydow, DS-GVO, Art. 13 Rn. 8.
[14] Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 406.

wird überwiegend eine Erhebung nicht bei dem Betroffenen angenommen.[15] In den hier diskutierten Anwendungsfällen haben die Fotografierten ebenfalls in der Regel keinen Einfluss darauf, ob sie abgelichtet werden und nehmen davon regelmäßig auch keine Kenntnis. Hierin besteht auch gerade die Vergleichbarkeit mit der verdeckten Videoüberwachung.

Die Auffassung der Anwendbarkeit des Art. 14 DSGVO erscheint daher vorzugswürdig. Denn wird allein auf die Erreichbarkeit des Betroffenen für den Verantwortlichen abgestellt, so ergeben sich im Einzelfall auch erhebliche Abgrenzungsschwierigkeiten.[16]

Es ist daher überzeugender, das Fotografieren von großen Menschenmengen oder Menschen als Beiwerk von Sehenswürdigkeiten nach Art. 14 DSGVO zu beurteilen.

Gemäß Art. 14 Abs. 5 lit. b Var. 1 und 2 DSGVO besteht eine Informationspflicht nicht, wenn die Erteilung der Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Die Unterscheidung der beiden Ausnahmetatbestände fällt in diesem Fall nicht leicht, da die Personen für den Fotografen zwar zum Zeitpunkt der Aufnahme potenziell erreichbar sein können, allerdings nur für einen kurzen Zeitpunkt und bei einer großen Anzahl von Menschen realistischer Weise auch nicht bezüglich aller Betroffenen. Weiterhin ist es dem einzelnen Fotografen im Regelfall auch nicht möglich, die Personen später zu identifizieren, da er nicht über die entsprechenden Mittel und insbesondere die Datenbanken hierzu verfügt. Die Personenbeziehbarkeit besteht also nur abstrakt – was i.R.d. Art. 4 Ziff. 1 DSGVO ausreicht[17] - konkret wird die Nutzung dieser abstrakten Möglichkeit allerdings im Regelfall ausscheiden. Es ist insoweit ein anderer Maßstab anzulegen, als bei der Frage, ob es sich bei den Bildern generell um personenbezogene Daten handelt. Dies ergibt sich daraus, dass es sich bei Art. 14 Abs. 5 lit. b um eine Einzelfallabwägung handelt, bei der auf die individuellen Gegebenheiten Bezug genommen werden kann. Da die

[15] BeckOK Datenschutzrecht/ Schmidt-Wudy, Art. 14 DSGVO Rn. 31.2.
[16] Ist eine Person auf der gegenüberliegenden Tribüne in einem Fußballstadion für den Fotografen erreichbar? Wäre dies anders zu beurteilen, wenn die Person auf der Nachbartribüne oder im gleichen Block sitzt?
[17] Siehe Seiten 2 und 3.

Personenbeziehbarkeit für den einzelnen Fotografen im Regelfall nicht möglich ist, ist auch die Information der Betroffenen im Regelfall als unmöglich anzusehen.

Ist es dem Fotografen im Einzelfall dennoch möglich, einzelne Personen zu identifizieren, so ist der Maßstab, ob eine Information dieser Person einen unverhältnismäßigen Aufwand erfordern würde. Hierbei ist dann der Aufwand mit dem Informationsinteresse des Betroffenen abzuwägen.[18]

IV. Ergebnis

Die derzeitige Rechtslage in Bezug auf Fotografien einer unüberschaubaren Anzahl von Menschen oder von Menschen als Beiwerk anderer Motive ist überwiegend unsicher. Dies beruht insbesondere darauf, dass der deutsche Gesetzgeber bisher keinen ausdrücklichen Gebrauch von der Öffnungsklausel des Art. 85 Abs. 2 DSGVO gemacht hat. Dies wäre aber im Sinne der Rechtssicherheit nötig.

Bis dahin ist es möglich, die Datenerhebung in den meisten Fällen über Art. 6 Abs. 1 lit. f DSGVO zu rechtfertigen. Eine Informationspflicht gegenüber den Abgelichteten besteht nicht. Dies ergibt sich aus Art. 11 Abs. 1 DSGVO, hilfsweise aus Art. 14 Abs. 5 lit. b DSGVO.

[18] Bäcker, in: Kühling/Buchner, DS-GVO, Art. 14 Rn. 55.

15.11.2018

Data-Breach-Meldungen nach Art. 33 DSGVO

Sogenannte Data Breaches sind unter Umständen der Aufsichtsbehörde und ggfs. auch den Betroffenen anzuzeigen. Die Meldung bei uns sollte unter Verwendung des Online-Formulars unter https://datenschutz-hamburg.de/meldung-databreach erfolgen, kann aber auch auf jedem sonstigen Weg in Textform eingereicht werden.

1. Meldepflichtiger Data Breach

Art. 33 DSGVO statuiert eine Meldepflicht bei der jeweils zuständigen Aufsichtsbehörde im „Falle einer Verletzung des Schutzes personenbezogener Daten“, „es sei denn, dass die Verletzung (…) voraussichtlich nicht zu einem Risiko führt“.

a) Verletzung des Schutzes personenbezogener Daten

Die Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DSGVO legaldefiniert als eine „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Es kommt nicht mehr – wie unter der vorherigen Rechtslage – darauf an, ob Daten von besonderen Kategorien betroffen sind. Jede Art personenbezogener Daten ist umfasst.

Die deutsche Formulierung „Verletzung des Schutzes“ darf nicht dahingehend missverstanden werden, dass jede Datenschutzverletzung (also jedes rechtswidrige Verhalten) zu melden ist.[1] Die englischsprachige Formulierung „Data Breach“ ist dahingehend deutlicher, dass es sich um einen Sicherheitsbruch handeln muss, bei dem Daten unrechtmäßig Dritten offenbart werden oder infolge eines Sicherheitsbruchs gelöscht oder zeitweise unzugänglich gemacht werden. Mögliche Beispiele sind Hacking und Datendiebstahl[2] sowie SQL-Lücken, Bugs im Webserver,

[1] *Martini*, in: Paal/Pauly, DSGVO, Art. 33 Rn. 16.
[2] *Hladjik*, in: Ehmann/Selmayr, DSGVO, Art. 33 Rn. 5.

verlorengegangene USB-Sticks oder Laptops, unrechtmäßige Übermittlung sowie der Einbruch in Serverräume, die mit dem Verlust oder der Zerstörung von Hardware oder dem Auslesen von Datenträgern einhergehen.[3]

Die „Verletzung der Sicherheit“ im Sinne des Art. 4 Nr. 12 DSGVO bedeutet nach überwiegender Literaturauffassung nicht die Unzulässigkeit der Datenverarbeitung, sondern betrifft die Datensicherheit, die nur durch technische und organisatorische Maßnahmen erreicht werden kann.[4] Die Art.-29-Gruppe erkennt an, dass es um „security incidents“ geht[5], nimmt zum Teil auch Fälle der rechtswidrigen Datenübermittlung als Verletzung der Sicherheit an, wenn dadurch eine Offenlegung an Dritte erfolgt. Das Gremium definiert den Begriff „Sicherheit“ zwar nicht, nennt aber unter anderem die Beispiele der versehentlichen Falsch-Adressierung von Briefen und E-Mails sowie die Versendung einer Massen-E-Mail unter Verwendung des cc- statt des bcc-Feldes (siehe Beispiele unten).[6] Entscheidend ist also für das Gremium, dass die Daten Dritten zu Kenntnis gegeben werden. Dies kann auch durch menschliches Versagen geschehen, das eine unzulässige Datenverarbeitung auslöst.[7] Die Auslegung der Art.-29-Gruppe ist für die Datenschutz-Aufsichtsbehörden bindend, da die Working Papers dieses Vorgängergremiums vom Europäischen Datenschutzausschuss in dessen erster Sitzung adaptiert wurden. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit folgt daher der Auffassung, dass auch versehentliche Falschadressierungen einen meldepflichtigen Vorgang darstellen, sofern davon ein Risiko für die Betroffenen ausgeht.

Neu ist die Meldepflicht auch bei vorübergehender Unerreichbarkeit der Daten oder dauerhafter Löschung infolge eines Sicherheitsbruchs. Dies setzt eine längere Dauer voraus und kann z.B. hervorgerufen werden durch einen Stromausfall oder durch eine Denial-of-Service-Attacke.[8] Geplante Systemausschaltungen fallen nicht darunter, vielmehr sind nur unbeabsichtigte Zugangshindernisse Data Breaches im Sinne des Art. 33 DSGVO.[9]

Der Verletzungserfolg muss eingetreten sein.[10] Der Erfolg ist etwa der – beabsichtigte oder unbeabsichtigte – Zugriff auf die Daten.[11] Nicht erforderlich ist hingegen eine Kenntnisnahme des

---

[3] *BayLDA*, Diskussionspapier zu Art. 33 und Art. 34 DSGVO v. 19.9.2016, S. 1.
[4] *Jandt*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 4 Nr. 12 Rn. 3 f.; *Klabunde*, in: Ehmann/Selmayr, DSGVO, Art. 4 Rn. 39; *Schild*, in: BeckOK DSGVO, Art. 4 Rn. 133.
[5] *Art.-29-Gruppe*, WP 250, S. 7; abrufbar unter https://datenschutz-hamburg.de/assets/pdf/wp250rev01_enpdf.pdf.
[6] *Art.-29-Gruppe*, WP 250, S. 32 f.; ebenso *Sassenberg*, in: Sydow, DSGVO, 2017, Art. 33 Rn. 18.
[7] Vgl. *Art.-29-Gruppe*, WP 250, S. 7.
[8] *Art.-29-Gruppe*, WP 250, S. 7.
[9] *Art.-29-Gruppe*, WP 250, S. 7.
[10] *Brink*, in: BeckOK DSGVO, Art. 33 Rn. 27; *Jandt*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7; *Martini*, in: Paal/Pauly, DSGVO, Art. 33 Rn. 16a.

Inhalts.[12] Fand trotz Bestehens einer Sicherheitslücke kein unberechtigter Zugriff statt, besteht keine Meldepflicht.[13] Für das Vorliegen einer Meldepflicht ist es unerheblich, ob daraufhin auch ein (Vermögens- oder immaterieller) Schaden eingetreten ist.[14] Das kann aber bei der Frage des Risikos Berücksichtigung finden.

b) Risiko

Das Risiko bemisst sich aus der Korrelation zwischen Schwere des Schadens und dessen Eintrittswahrscheinlichkeit.[15] Je höher der anzunehmende Schaden ist, desto geringer sind die Anforderungen an die Wahrscheinlichkeit seines Eintritts.[16] Die Art.-29-Gruppe sieht bei der Risikobetrachtung die folgenden Kriterien vor[17]:

- Art des Data Breach (Unautorisierter Zugriff ist oft gravierender als Datenverlust)
- Art und Umfang der Daten
- Identifizierbarkeit (Wie einfach und wahrscheinlich ist es, dass ein Dritter, der unautorisierten Zugriff nimmt, den Personenbezug herstellen kann?)
- Spezielle Umstände hinsichtlich der Betroffenen (z.B. Kinder, Behinderungen)
- Spezielle Umstände hinsichtlich des Verantwortlichen (z.B. medizinische Einrichtung)
- Anzahl der Betroffenen
- Zu erwartende Konsequenzen. Zu den Konsequenzen nennt EG 85 typische Fallgruppen:
    - Verlust der Kontrolle über die eigenen Daten
    - Einschränkung von Rechten
    - Diskriminierung
    - Identitätsdiebstahl oder -betrug
    - Finanzielle Verluste
    - Aufhebung der Pseudonymisierung
    - Rufschädigung
    - Verletzung des Berufsgeheimnisses
    - Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

2. Information der Betroffenen

Zusätzlich zur Meldung bei der Aufsichtsbehörde muss der Verantwortliche in manchen Fällen auch die betroffenen Personen informieren. Die Informationspflicht nach Art. 34 Abs. 1 DSGVO besteht, wenn der Data Breach „voraussichtlich ein hohes Risiko für die persönlichen Rechte

[11] *Reif*, in: Gola, DSGVO, Art. 33 Rn. 21.
[12] *Sassenberg*, in: Sydow, DSGVO, 2017, Art. 33 Rn. 7.
[13] *Reif*, in: Gola, DSGVO, Art. 33 Rn. 21.
[14] *Jandt*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7.
[15] *Jandt*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7; *Martini*, in: Paal/Pauly, DSGVO, Art. 33 Rn. 23 f.
[16] *Brink*, in: BeckOK DSGVO, Art. 33 Rn. 36.
[17] *Art.-29-Gruppe*, WP 250, S. 24 f.

und Freiheiten“ zur Folge hat. Im Gegensatz zu Art. 33 setzt Art. 34 also nicht nur ein Risiko, sondern ein hohes Risiko voraus. Die unter 1.b) genannten Kriterien und Fallgruppen greifen auch hier.[18] Darüber hinaus sind die Ausnahmen von der Informationspflicht gem. Art. 34 Abs. 3 DSGVO zu beachten.

3. Beispiele

Das WP 250 der Art.-29-Gruppe enthält in Anhang B einige Beispiele, die nachfolgend zusammengefasst wiedergegeben werden.

Fallbeschreibung	Meldepflicht an die Aufsichtsbehörde	Informationspflicht an Betroffene	Anmerkungen
Gestohlener USB-Stick mit wirksam verschlüsselten Daten	Nein	Nein	Kein Art.-33-Fall aufgrund der Verschlüsselung. Meldepflicht besteht jedoch, wenn die Daten nicht anderweitig gesichert sind.
Datenzugriff durch Cyber-Attacke	Ja	Ja (abhängig von der Art der Daten)	
Mehrminütiger Stromausfall, dadurch zwischenzeitlich kein Zugriff möglich	Nein	Nein	Aber interne Dokumentation nach Art. 33 Abs. 5
Ransomware-Attacke, die Kundendaten verschlüsselt (Erpressungstrojaner)	Ja (in der Regel)	Ja (in der Regel)	Außer es gibt ein Backup, sodass die Daten zügig wiederhergestellt werden können.
Kontoauszug an falschen Kunden verschickt	Ja	Im Einzelfall i.d.R. nicht, bei Häufung schon	

[18] Vgl. *Art.-29-Gruppe*, WP 250, S. 9.

Hacker erbeuten Nutzernamen, Passwörter und Kaufhistorie der Kunden eines Onlineshops	Ja	Ja	
Kunden können aufgrund eines Programmierfehlers im Kundenportal fremde Kundendaten einsehen	Ja, wenn Daten abgerufen wurden	Kommt darauf an	
Cyber-Attacke auf Krankenhaus, dadurch für 30 Minuten kein Zugriff auf Patientendaten	Ja	Ja	
Versehentliche Versendung von Schülerdaten an eine Mailingliste	Ja	Ja (in der Regel)	
Werbe-E-Mail mit offenem Mailverteiler (cc statt bcc)	Ja (bei großer Empfängerzahl oder sensiblem Inhalt, z.B. Passwörter)	Ja (außer nur wenige Betroffene und kein sensibler Inhalt)	

4. Rechtzeitigkeit der Meldung

Die Meldung muss unverzüglich, spätestens nach 72 Stunden bei der Aufsichtsbehörde eingehen. Die Frist beginnt ab Kenntnis von den erheblichen Tatsachen durch die verantwortliche Stelle. Dabei genügt es grundsätzlich, dass jemand im Unternehmen oder der Behörde Kenntnis erlangt. Wenn die Meldung nach „allgemeinem Ermessen“ früher möglich ist, hat sie früher zu erfolgen (EG 86). Wird die 72-Stunden-Frist nicht gehalten, hat der Verantwortliche dies zu begründen (Art. 33 Abs. 1 Satz 2 DSGVO). Dabei müssen außergewöhnliche Umstände dargelegt werden.[19] Ein akzeptabler Grund liegt z.B. vor, wenn viele Hacker-Attacken in kurzem Zeitraum auftreten.[20]

[19] Vgl. *Art.-29-Gruppe*, WP 250, S. 16.
[20] *Art.-29-Gruppe*, WP 250, S. 16.

Kenntnis ist dann erlangt, wenn der Verantwortliche mit einen angemessenen Grad an Sicherheit davon auszugehen hat, dass ein Data Breach vorliegt.[21] Die Meldepflicht tritt demnach noch nicht ein, wenn zunächst nur vage Hinweise vorliegen. Dann hat die Stelle so schnell wie möglich weitere Ermittlungen anzustellen. Während der Ermittlungsphase liegt noch kein angemessener Grad an Sicherheit an Kenntnis über das Vorliegen eines Data Breach vor.[22] Der Verantwortliche muss die Meldung vornehmen, sobald sich in den Ermittlungen ein angemessener Grad an Sicherheit herauskristallisiert[23], also gegebenenfalls schon bevor der Sachverhalt vollständig ausermittelt ist. Ein angemessener Grad an Sicherheit liegt z.B. vor, wenn ein USB-Stick mit unverschlüsseltem Inhalt verloren gegangen ist, obwohl nicht nachvollzogen werden kann, ob Dritte die Daten ausgelesen haben.[24] Wenn der Verantwortliche einen Hinweis inklusive eines Beweises erhält, hat er ebenfalls Kenntnis[25], nicht jedoch, wenn der Hinweis zu unsubstantiiert ist und weitere Ermittlungen notwendig sind. Leitet beispielsweise ein Betroffener eine Phishing-Mail an den Verantwortlichen weiter, die Kundendaten des Verantwortlichen enthält, so hat der Verantwortliche nicht in jedem Fall sofort eine Meldung abzusetzen. Zunächst hat er sein System auf unautorisierte Zugriffe zu überprüfen und hat erst dann Kenntnis, wenn er solche Zugriffe entdeckt.[26] Der Umfang der Meldung bestimmt sich nach Art. 33 Abs. 3 DSGVO.

Sind noch nicht alle vom Gesetz geforderten Inhalte bekannt (z.B. Datenkategorien oder Anzahl der Betroffenen), ist dies kein Hinderungsgrund für eine rechtzeitige Meldung.[27] Dann hat die Meldung schrittweise zu erfolgen (Art. 33 Abs. 4 DSGVO), sodass die fehlenden Informationen später nachgereicht werden.

[21] *Art.-29-Gruppe*, WP 250, S. 11.
[22] *Art.-29-Gruppe*, WP 250, S. 11.
[23] *Art.-29-Gruppe*, WP 250, S. 11.
[24] *Art.-29-Gruppe*, WP 250, S. 11.
[25] *Art.-29-Gruppe*, WP 250, S. 11.
[26] Vgl. *Art.-29-Gruppe*, WP 250, 11.
[27] *Art.-29-Gruppe*, WP 29, S. 14.

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

---

[1] See Article 4(21) of the GDPR

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

[7] See Articles 34(4) and 58(2)(e)

Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.

I. Personal data breach notification under the GDPR

A. Basic security considerations

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

---

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).

[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] See Articles 5(1)(f) and 32.

[11] Article 32; see also Recital 83

[12] See Recital 87

B. What is a personal data breach?

1. Definition

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a "personal data breach" in Article 4(12) as:

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Example

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].

The potential adverse effects of a breach on individuals are considered below.

2. Types of personal data breaches

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access[15] to, or destruction of, personal data.

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

[14] See Opinion 03/2014

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information,"

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12).

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

Examples

available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: " Timely, reliable access to data and information services for authorized users." See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] See Article 33(5)

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

3. The possible consequences of a personal data breach

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[17].

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is

[17] See also Recitals 85 and 75

[18] See also Recital 86.

presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state: "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

II. Article 33 - Notification to the supervisory authority

A. When to notify

1. Article 33 requirements

Article 33(1) provides that:

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Recital 87 states[20]:

> "It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

2. When does a controller become "aware"?

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Recital 85 is also important here.

controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact

[21] See Recital 87

assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

Example

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach.
- Documentation of the breach should take place as it develops.

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

3. Joint controllers

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

4. Processor obligations

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends the

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] See also Recital 79.

processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.

B. Providing information to the supervisory authority

1. Information to be provided

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:

> "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

Article 33(3) states that the controller "shall at least" provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

Example

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

In any event, the supervisory authority may request further details as part of its investigation into a breach.

2. Notification in phases

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states:

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the

[26] See Article 9.

breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

Example

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

3. Delayed notifications

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

C. Cross-border breaches and breaches at non-EU establishments

1. Cross-border breaches

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that:

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."

However, Article 56(1) states:

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

Furthermore, Article 56(6) states:

> "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

2. Breaches at non-EU establishments

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]:

---

[27] See Article 4(23)

[28] See also Recital 122.

[29] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] See also Recitals 23 and 24

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Article 3(3) is also relevant and states[32]:

"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).

D. Conditions where notification is not required

Article 33(1) makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

[32] See also Recital 25

[33] See Recital 80 and Article 27

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] See also Article 4(1) and (2) of Regulation 611/2013.

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Example

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

III. **Article 34 – Communication to the data subject**

A. Informing individuals

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) states:

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

B. Information to be provided

When notifying individuals, Article 34(2) specifies that:

> "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."

According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

[36] See also Recital 86.

C. Contacting individuals

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

At the same time, Recital 86 explains that:

> "Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

D. Conditions where communication is not required

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

IV. Assessing risk and high risk

A. Risk as a trigger for notification

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] See Article 5(2)

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

B. Factors to consider when assessing risk

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

[39] See Recital 75 and Recital 85.

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]:

- The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- The nature, sensitivity, and volume of personal data

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- Ease of identification of individuals

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- Severity of consequences for individuals.

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal

data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].

V. Accountability and record keeping

A. Documenting breaches

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains:

> "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with Article 83.

B. Role of the Data Protection Officer

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

---

[44] See Article 5

[45] See Article 6 and also Article 9.

[46] See Article 5(1)(e).

[47] See Recital 85

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

VI. Notification obligations under other legal instruments

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

51 Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*

GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).

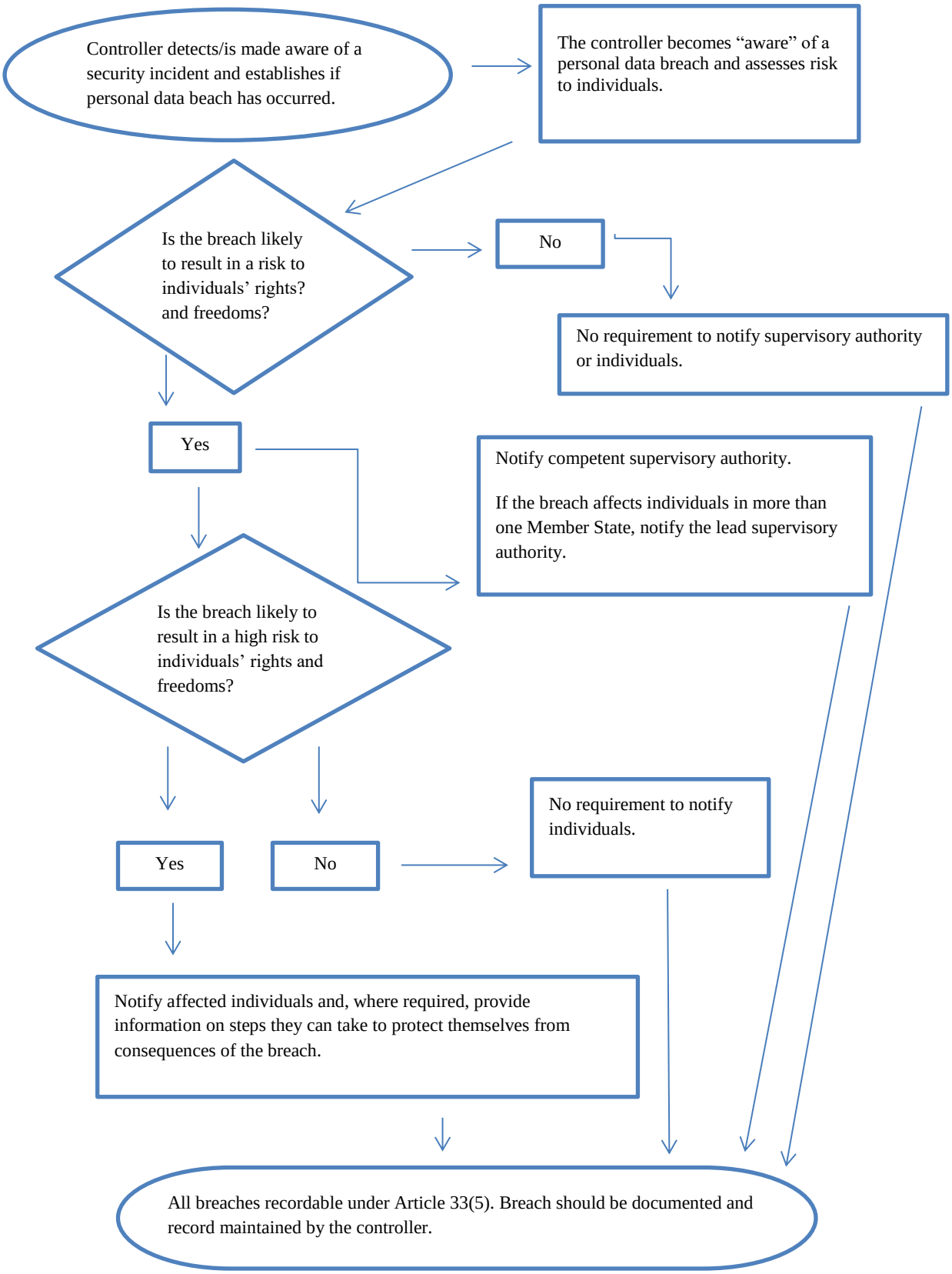
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52] must notify breaches to the competent national authorities.

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Annex**

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	**Notify the supervisory authority?**	**Notify the data subject?**	**Notes/recommendations**
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

functionality was to encrypt the data, and that there was no other malware present in the system.		consequences.	confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which	As the processor, the website hosting company must notify its affected clients (the controllers) without	If there is likely no high risk to the individuals they do not need to be	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS

controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	notified.	Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.