GIBSON DUNN

Ronald O. Mueller
Partner
T: +1 202.955.8671
rmueller@gibsondunn.com

January 20, 2025

VIA ONLINE PORTAL SUBMISSION

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: *Amazon.com, Inc.*
Shareholder Proposal of Mercy Investment Services, Inc., et al.
Securities Exchange Act of 1934—Rule 14a-8

Ladies and Gentlemen:

This letter is to inform you that our client, Amazon.com, Inc. (the "Company"), intends to omit from its proxy statement and form of proxy for its 2025 Annual Meeting of Shareholders (collectively, the "2025 Proxy Materials") a shareholder proposal (the "Proposal") and statement in support thereof (the "Supporting Statement") received from Mercy Investment Services, Inc.; the Northwest Women Religious Investment Trust; Miller/Howard Investments, Inc. on behalf of Eva Horowitz; Missionary Oblates of Mary Immaculate, US Province; the Durocher Fund; CommonSpirit Health; and the Adrian Dominican Sisters (collectively, the "Proponents").

Pursuant to Rule 14a-8(j), we have:

- filed this letter with the Securities and Exchange Commission (the "Commission") no later than eighty (80) calendar days before the Company intends to file its definitive 2025 Proxy Materials with the Commission; and

- concurrently sent copies of this correspondence to the Proponents.

Rule 14a-8(k) and Staff Legal Bulletin No. 14D (Nov. 7, 2008) ("SLB 14D") provide that shareholder proponents are required to send companies a copy of any correspondence that the proponents elect to submit to the Commission or the staff of the Division of Corporation Finance (the "Staff"). Accordingly, we are taking this opportunity to inform the Proponents that if the Proponents elect to submit additional correspondence to the Commission or the Staff with respect to the Proposal, a copy of such correspondence should be furnished concurrently to the undersigned on behalf of the Company pursuant to Rule 14a-8(k) and SLB 14D.

THE PROPOSAL

The Proposal states:

> **RESOLVED,** that shareholders of Amazon Inc. ("Amazon") urge the board of directors to oversee an independent Data Protection Impact Assessment[1] on the company's healthcare service offerings that describes how the company is ensuring appropriate use of, and informed consent for collection of, patient data. The assessment should cover Amazon OneMedical [*sic*] and Amazon Pharmacy, be prepared at reasonable cost and omitting confidential and proprietary information and be made available on Amazon's web site.

A copy of the Proposal and the Supporting Statement is attached to this letter as Exhibit A.

BASES FOR EXCLUSION

We hereby respectfully request that the Staff concur in our view that the Proposal may be excluded from the 2025 Proxy Materials pursuant to:

- Rule 14a-8(i)(3) because the Proposal is impermissibly vague and indefinite so as to be inherently misleading; and
- Rule 14a-8(i)(7) because the Proposal relates to the Company's ordinary business operations and seeks to micromanage the Company.

ANALYSIS

I. The Proposal May Be Excluded Under Rule 14a-8(i)(3) Because The Proposal Is Impermissibly Vague And Indefinite So As To Be Inherently Misleading.

Rule 14a-8(i)(3) permits the exclusion of a shareholder proposal if the proposal or supporting statement is contrary to any of the Commission's proxy rules, including Rule 14a-5(a), which requires information in a proxy statement to be clearly presented, and Rule 14a-9, which prohibits materially false or misleading statements in proxy soliciting materials.

In Staff Legal Bulletin No. 14B (Sept. 15, 2004), the Staff confirmed that a proposal may properly be excluded pursuant to Rule 14a-8(i)(3) when the proposal and supporting statement, when read together, are "so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." *See New York City Employees' Retirement System v. Brunswick Corp.*, 789 F. Supp.

[1] https://gdpr.eu/data-protection-impact-assessment-template/.

144, 146 (S.D.N.Y. 1992) (proposal "lacks the clarity required of a proper shareholder proposal"; "Shareholders are entitled to know precisely the breadth of the proposal on which they are asked to vote"); *Dyer v. SEC*, 287 F.2d 773, 781 (8th Cir. 1961) ("it appears to us that the proposal, as drafted and submitted to the company, is so vague and indefinite as to make it impossible for either the board of directors or the stockholders at large to comprehend precisely what the proposal would entail"); *Capital One Financial Corp.* (avail. Feb. 7, 2003) (concurring with the exclusion under Rule 14a-8(i)(3) of a proposal where the company argued that its shareholders "would not know with any certainty what they are voting either for or against"). As further described below, the Proposal is so vague and indefinite that neither the Company nor the Company's shareholders can comprehend with any level of certainty what the Proposal would entail and, therefore, the Proposal is excludable under Rule 14a-8(i)(3).

Here, the Proposal is vague and misleading in numerous material aspects, to such a degree that neither shareholders nor the Company would know what actions the Proposal requires. Specifically, the Proposal requests "an independent Data Protection Impact Assessment on the company's healthcare service offerings that describes how the [C]ompany is ensuring appropriate use of, and informed consent for collection of, patient data." The Supporting Statement discusses various patient data privacy considerations, and concludes by stating, "An assessment that discloses information about how the [C]ompany is ensuring patients are informed about what data is collected and how it will be used, would mitigate reputational, financial and legal risk from Amazon's commercial healthcare offerings." As noted, however, the Proposal specifically calls for a "Data Protection Impact Assessment," and the Resolved clause includes a footnote to a website describing Data Protection Impact Assessments ("DPIAs") under the General Data Protection Regulation (the "GDPR") and further linking to a DPIA template.[2] As the name suggests, a "Data Protection Impact Assessment" is a process provided for under the EU and UK's GDPR that is oriented to assessing the *data protection* risks of an operation (i.e., protecting information from unauthorized use) and is not designed for conducting a general assessment of compliance with *data privacy* standards (which focus on who is authorized to use information and for what purposes).[3] In addition, the Proposal references Amazon One Medical and Amazon Pharmacy, yet those offerings are limited to the U.S. and are not subject to the GDPR.

The DPIA's focus on data protection is reflected on the website linked in the Proposal, which states that the GDPR requires DPIAs to contain the following elements, each of which are

---

[2] *See* https://gdpr.eu/data-protection-impact-assessment-template/.

[3] *See, e.g.*, the UK's Information Commissioner's Office discussion of Data Protection Impact Assessments at https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias-1-0.pdf, stating, "A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks." *See also* Forbes, *Data Privacy Vs. Data Protection: Understanding The Distinction In Defending Your Data* (last updated Dec. 10, 2021), *available at* https://www.forbes.com/councils/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/ ("Data protection is focused on protecting assets from unauthorized use, while data privacy defines who has authorized access.").

focused on how data is handled and processed, not on how consent is obtained for the collection of data or on how the data is utilized:

- "A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller"
- "An assessment of the necessity and proportionality of the processing operations in relation to the purposes"
- "An assessment of the risks to the rights and freedoms of data subjects"
- "The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned"

Similarly, the DPIA template linked at the website cited in the Proposal[4] is focused on data protection questions assessing the collection, processing, purpose, storage, and deletion of data, not on processes around obtaining consent and informing data subjects about how data is used. *See* Exhibit B. Thus, while data privacy, informed consent, and appropriate use of personal data are aspects of the GDPR and may be indirectly touched upon or implicated by a DPIA, the evaluation called for under a DPIA is not oriented to assessing data privacy, informed consent, and appropriate use of personal data, and thus is inapposite to "ensuring patients are informed about what data is collected and how it will be used," as requested in the Proposal and Supporting Statement. Thus, it is misleading, or at least vague and confusing, to propose that the Company assess data privacy considerations through a DPIA, which is designed to assess *data protection*, and the Proposal and Supporting Statement do not explain how the Company would be expected to do so.

Other aspects of DPIAs further make it unclear how such an assessment is to be conducted as requested in the Proposal. For example, under the GDPR, a DPIA is to be carried out prior to conducting any processing of personal data. As stated on the website cited in the Proposal,[5] "You must prepare your DPIA before beginning any data processing activity. Ideally, you should conduct your DPIA before and during the planning stages of your new project." In contrast, the Proposal states that the DPIA "should cover Amazon OneMedical [*sic*] and Amazon Pharmacy," which are businesses that are already in operation and thus already collect and process customer data. In addition, Amazon One Medical and Amazon Pharmacy are available to customers in the U.S. as part of Amazon Health Services ("AHS"), a U.S. business unit focused only on U.S. customers and, as noted above, not subject to the GDPR. The Company has designed AHS's operations, including its data collection and use standards and disclosures, to

[4] https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

[5] *See* note 2, *supra*.

comply with numerous applicable U.S. federal and state laws. In contrast, a DPIA is designed to assess compliance with the GDPR, and the GDPR "imposes obligations onto organizations anywhere, so long as they target or collect data *related to people in the EU*" (emphasis added).[6]

As such, the Proposal is vague and misleading because it is unclear how the Company would be expected to conduct a retroactive assessment of data privacy (including appropriate data use and customer consent) through a data protection assessment that is supposed to be conducted in advance and is oriented to an assessment under laws that are not applicable to the business operations that are the subject of the Proposal.

The Staff has routinely concurred with the exclusion of proposals that fail to provide sufficient clarity or guidance to enable either shareholders or the company to understand how the proposal would be implemented. For example, in *Apple Inc. (Zhao)* (avail. Dec. 6, 2019) ("*Apple (Zhao)*"), the Staff concurred that a company could exclude, as vague and indefinite, a proposal that recommended that the company "improve guiding principles of executive compensation," but failed to define or explain what improvements the proponent sought to the "guiding principles." The Staff noted that the proposal "lack[ed] sufficient description about the changes, actions or ideas for the [c]ompany and its shareholders to consider that would potentially improve the guiding principles" and concurred with exclusion of the proposal as "vague and indefinite." Similarly, in *The Walt Disney Co. (Grau)* (avail. Jan. 19, 2022) ("*Walt Disney (Grau)*"), the Staff concurred with the exclusion under Rule 14a-8(i)(3) of a proposal requesting a prohibition on communications by or to cast members, contractors, management or other supervisory groups within the company of "politically charged biases regardless of content or purpose," where the Staff stated that "in applying this proposal to the [c]ompany, neither shareholders nor the [c]ompany would be able to determine with reasonable certainty exactly what actions or measures the [p]roposal requests." *See also The Boeing Co.* (avail. Feb. 23, 2021) (concurring with the exclusion under Rule 14a-8(i)(3) of a proposal requiring that 60% of the company's directors "must have an aerospace/aviation/engineering executive background" where such phrase was undefined); *AT&T Inc.* (avail. Feb. 21, 2014) (concurring with the exclusion under Rule 14a-8(i)(3) of a proposal requesting a review of policies and procedures related to the "directors' moral, ethical and legal fiduciary duties and opportunities," where such phrase was undefined); *Puget Energy, Inc.* (avail. Mar. 7, 2002) (concurring with the exclusion under Rule 14a-8(i)(3) of a proposal requesting that the company's board of directors implement "a policy of improved corporate governance" where it also included a broad array of unrelated topics that could be covered by such a policy).

Similar to *Apple (Zhao)* and *Walt Disney (Grau)*, the central request of the Proposal—that the Company conduct a data protection assessment oriented toward EU/UK compliance standards to assess patient data privacy ("appropriate use of, and informed consent for collection of, patient data") for U.S. operations—is so ambiguous that it is impossible for the Company or shareholders "to determine with any reasonable certainty exactly what actions or measures the

[6] *See* GDPR, *available at* https://gdpr.eu/tag/gdpr/.

[P]roposal requires." As a result of the Proposal's lack of guidance or clarity on how these divergent concepts are to be reconciled and applied, shareholders would be unable to assess the scope and nature of the assessment they are being asked to support, and the Company would be unable to determine how to implement the Proposal. Accordingly, the Proposal's reference to a standard that is oriented to assessing data protection and that does not apply in the jurisdiction in which AHS collects and uses patient data causes the Proposal to be impermissibly vague and indefinite and renders it excludable under Rule 14a-8(i)(3).

II. The Proposal May Be Excluded Under Rule 14a-8(i)(7) Because The Proposal Relates To The Company's Ordinary Business Operations.

A. Background On The Ordinary Business Standard.

Rule 14a-8(i)(7) permits a company to omit from its proxy materials a shareholder proposal that relates to the company's "ordinary business" operations. According to the Commission's release accompanying the 1998 amendments to Rule 14a-8, the term "ordinary business" "refers to matters that are not necessarily 'ordinary' in the common meaning of the word," but instead the term "is rooted in the corporate law concept providing management with flexibility in directing certain core matters involving the company's business and operations." Exchange Act Release No. 40018 (May 21, 1998) (the "1998 Release"). In the 1998 Release, the Commission stated that the underlying policy of the ordinary business exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting," and identified two central considerations that underlie this policy. *Id.* The first of those considerations is that "[c]ertain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight." The second consideration concerns "the degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." *Id.* (citing Exchange Act Release No. 12999 (Nov. 22, 1976)).

The Commission has stated that a proposal requesting the dissemination of a report is excludable under Rule 14a-8(i)(7) if the substance of the proposal is within the ordinary business of the company. *See* Exchange Act Release No. 34-20091 (Aug. 16, 1983) ("the staff will consider whether the subject matter of the special report or the committee involves a matter of ordinary business; where it does, the proposal will be excludable under Rule 14a-8(c)(7)"). *See Johnson Controls, Inc.* (avail. Oct. 26, 1999) ("[where] the subject matter of the additional disclosure sought in a particular proposal involves a matter of ordinary business . . . it may be excluded under [R]ule 14a-8(i)(7)"); *see also Ford Motor Co.* (avail. Mar. 2, 2004) (concurring with the exclusion of a proposal requesting that the company publish a report about global warming/cooling, where the report was required to include details of indirect environmental consequences of its primary automobile manufacturing business).

In the instant case, the Proposal relates to the Company's management and handling of patient data in the context of its AHS businesses, which are subject to the Company's obligation to comply with laws, rules, and regulations, and involve other core business considerations that routinely arise in managing the Company's operations. In addition, the Proposal would micromanage the Company by seeking to inappropriately limit management's discretion in addressing the complex issue of assessing and evaluating its management of patient data. As such, similar to the well-established precedents described in greater detail below and consistent with the Commission and Staff guidance and Staff precedents, the Proposal involves matters related to the Company's ordinary business and may be excluded under Rule 14a-8(i)(7).

B. The Proposal May Be Excluded Because Its Subject Matter Relates To The Terms Upon Which The Company Offers Its Products And Services To Customers, Including How The Company Manages Customer Data.

The Proposal seeks to require that the Company oversee an independent DPIA that "describes how the [C]ompany is ensuring appropriate use of, and informed consent for collection of, patient data." The Company's decision-making regarding the policies and procedures that govern the Company's collection and use of patient data and the terms upon which AHS's services are offered to its U.S. customers implicate routine management decisions that encompass legal, regulatory, operational, risk management, and financial considerations, among others. For example, as a participant in the healthcare industry in the U.S., AHS is already highly regulated, including by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which, among other things, includes provisions addressing collection and use of various types of patient data, such as medication history, medical conditions, treatment information, and health insurance information. In addition, the Company is required to comply with U.S. federal and state privacy and security laws, including regulations and restrictions on the collection, use, and disclosure of medical information. As a result, the Company has developed a detailed set of policies and procedures encompassing the handling of patient data, including policies and procedures consistent with applicable federal, state, and local regulatory requirements, and this is reflected in the terms of service and privacy notices of its AHS businesses. The Proposal impermissibly seeks to interject shareholders into this complex and core aspect of the Company's ordinary business.

The Staff has consistently concurred with the exclusion of proposals relating to how a company handles the terms upon which it offers products and services to its clients, particularly in highly regulated industries. For instance, in *Bank of America Corp. (National Center for Public Policy Research)* (avail. Feb. 29, 2024), the Staff concurred with exclusion under Rule 14a-8(i)(7) of a proposal requesting that the Company report "whether and to what extent [the company] requested that [c]ompany clients deny their products or services to certain customers or categories of customers, or has demanded such restrictions as a condition of [c]ompany's continuing to do business with said clients." The company argued that the proposal could be excluded as it related to the terms upon which the company offered its products to clients and, in particular, given that it had specific policies and procedures in place that were necessary to comply with the significant laws, rules, and regulations to which it was subject as a global

financial institution. Similarly, in *PayPal Holdings, Inc. (Laurent Ritter)* (avail. Apr. 10, 2023) ("*PayPal*"), the proposal requested that the board of directors revise its reporting to "provide clear explanations of the number and categories of account suspensions and closures that may reasonably be expected to limit freedom of expression or access to information or financial services" and the supporting statement requested that the report include the "external legal or policy basis and internal company criteria for removals," as well as "[a]ny efforts by the company to mitigate the harmful effects" of such account closures. The Staff concurred with the proposal's exclusion under Rule 14a-8(i)(7).

The Staff also has consistently concurred with the exclusion of proposals related specifically to the management of sensitive customer information in regulated industries. For instance, in *American Express Co.* (avail. Mar. 9, 2023), the Staff concurred with the exclusion under Rule 14a-8(i)(7) of a proposal requesting an evaluation and report "describing if and how the [c]ompany intends to reduce the risk associated with tracking, collecting, or sharing information regarding the processing of payments involving its cards and/or electronic payment system services for the sale and purchase of firearms." The supporting statement, like the Supporting Statement, raised concerns regarding the management of sensitive customer information in a highly regulated industry, specifically "the privacy of gun ownership" in the financial services industry. Similarly, in *AT&T Inc.* (avail. Jan. 30, 2017) ("*AT&T 2017*"), the proposal requested that the board "review and publicly report . . . on the consistency between AT&T's policies on privacy and civil rights and the [c]ompany's actions with respect to U.S. law enforcement investigations." The supporting statements, like the Supporting Statement, raised concerns regarding how sensitive information from a company in a regulated industry could be used inappropriately, specifically, "how cooperation between U.S. law enforcement entities and telecommunications companies affects Americans' privacy and civil rights." The Staff concurred with the proposal's exclusion under Rule 14a-8(i)(7), noting it "relate[d] to procedures for protecting customer information." This was also the Staff's conclusion in *AT&T Inc.* (avail. Feb. 5, 2016) ("*AT&T 2016*"), where the proposal requested that the company "issue a report . . . clarifying the [c]ompany's policies regarding providing information to law enforcement and intelligence agencies, domestically and internationally, above and beyond what is legally required . . . , whether and how the policies have changed since 2013, and assessing risks to the [c]ompany's finances and operations arising from current and past policies and practices." The Staff concurred that the proposal related to "procedures for protecting customer information and [did] not focus on a significant policy issue." *See also AT&T Inc.* (avail. Feb. 7, 2008) (concurring with the exclusion under Rule 14a-8(i)(7) of a proposal requesting that the company's board of directors prepare a report discussing, from technical, legal, and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to governmental agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers because it related to the company's "ordinary business operations (i.e., procedures for protecting customer information)").

The foregoing precedents are consistent with the position that proposals relating to the terms upon which a company offers its products or services, including terms related to a company's

practices for handling customer information, can be excluded pursuant to Rule 14a-8(i)(7) as relating to the company's ordinary business operations, particularly when the practices are related to sensitive information in a regulated industry. Here, like the policies, practices, and procedures at issue in *American Express*, *AT&T 2017*, and the other precedents cited above, the Proposal relates to the Company's day-to-day management and handling of sensitive customer information, as it requests that the Company oversee an independent assessment "on the [C]ompany's healthcare service offerings that describes how the [C]ompany is ensuring appropriate use of, and informed consent for collection of, patient data." The Proposal thus involves decisions regarding the Company's terms of service related to its AHS business, which is a fundamental responsibility of management as it requires consideration of numerous factors that the Company must manage as part of its ordinary business operations. These considerations involve complex evaluations, including designing customer account terms and information systems that allow the Company to comply with laws, rules, and regulations, which shareholders are not suited to oversee or direct through the shareholder proposal process. Balancing such considerations is a complex matter and is "so fundamental to management's ability to run a company on a day-to-day basis that [it] could not, as a practical matter, be subject to direct shareholder oversight." *See* 1998 Release. Like in *Bank of America*, where the terms upon which the company, a global financial institution, offered its products to clients were subject to significant regulation, here, policies and procedures related to patient data are influenced by various legal, regulatory, operational, risk management, and financial considerations, among others. As such, consistent with Staff precedents, the Proposal, by attempting to subject the Company's policies and procedures surrounding the management and handling of patient data to shareholder oversight and a shareholder vote, addresses issues that are ordinary business matters for the Company, and is therefore properly excludable under Rule 14a-8(i)(7).

C. The Proposal Is Excludable Because It Relates To The Company's General Legal Compliance.

As discussed in Section I above, the exact nature of the assessment requested by the Proposal is vague and misleading; however, the Proposal's reference to the GDPR DPIA template, as well as the Supporting Statement's references to HIPAA and enforcement actions by the Federal Trade Commission, indicate that the Proposal is primarily focused on compliance with legal requirements to "mitigate reputational, financial and legal risk from Amazon's commercial healthcare offerings"—issues that are core components of the Company's ordinary business operations.

The Staff has consistently concurred with the exclusion of proposals concerning a company's legal compliance program as relating to matters of ordinary business pursuant to Rule 14a-8(i)(7). *See, e.g.*, *Texas Pacific Land Corp. (Jason Hubert)* (avail. Sept. 5, 2023) (concurring with the exclusion under Rule 14a-8(i)(7) of a proposal requesting a review of a company's processes regarding the preparation of its Commission-filed proxy materials where the company argued that compliance with the proxy rules was part of its ordinary business); *Eagle Bancorp, Inc.* (avail. Mar. 29, 2022) (concurring with the exclusion under Rule 14a-8(i)(7) of a proposal

requesting an independent review of certain investigations performed by the company where the company argued that such investigations related to the company's legal compliance and related business and policy practices); *Navient Corp.* (avail. Mar. 26, 2015, *recon. denied* Apr. 8, 2015) (concurring with the exclusion of a proposal requesting "a report on the company's internal controls over student loan servicing operations, including a discussion of the actions taken to ensure compliance with applicable federal and state laws" as "concern[ing] a company's legal compliance program"); *Raytheon Co.* (avail. Mar. 25, 2013) (concurring with the exclusion of a proposal requesting a report on "the board's oversight of the company's efforts to implement the provisions of the Americans with Disabilities Act, the Fair Labor Standards Act, and the Age Discrimination in Employment Act" with the Staff noting that proposals concerning a company's legal compliance program are generally excludable under Rule 14a-8(i)(7)); *Sprint Nextel Corp.* (avail. Mar. 16, 2010, *recon. denied* Apr. 20, 2010) (concurring with the exclusion of a proposal requesting that the board explain why it has failed to adopt an ethics code designed to, among other things, promote securities law compliance since proposals relating to "adherence to ethical business practices and the conduct of legal compliance programs are generally excludable under [R]ule 14a-8(i)(7)"); *The Coca-Cola Co.* (avail. Jan. 9, 2008) (concurring with the exclusion of a proposal seeking an annual report comparing independent laboratory tests of the company's product quality against applicable national laws and the company's global quality standards because the proposal related to the ordinary business matter of the "general conduct of a legal compliance program"); *Halliburton Co.* (avail. Mar. 10, 2006) (concurring with the exclusion of a proposal requesting a report on policies and procedures to reduce or eliminate the reoccurrence of certain violations and investigations as relating to ordinary business operations "(i.e., general conduct of a legal compliance program)").

Recently, in *Exxon Mobil Corp. (Oxfam America)* (avail. Mar. 20, 2024), the Staff concurred with the exclusion under Rule 14a-8(i)(7) of a proposal requesting that the board issue a tax transparency report to shareholders with consideration of the guidelines set forth in the Global Reporting Initiative's Tax Standard (the "GRI Standard"). The company argued that not only was management of corporate taxation a legal compliance matter that "require[d] an intricate understanding of ever-changing tax regulations and tax regimes that [was] inappropriate for direct shareholder oversight," but also, given that the GRI Standard involved "complex corporate taxation matters," shareholders "would be unable to fully understand the Company's tax strategies and related risk assessments without the requisite knowledge of tax regulations and policies." Similarly, here, the Proposal requests an assessment on how the Company manages a particular aspect of its legal compliance program, specifically its collection and use of patient data. Just as the proposal in *Exxon Mobil* provides the GRI Standard as the guideline on which the requested report be prepared, the Proposal provides the GDPR DPIA template as the guideline on which the requested assessment be prepared.[7]

[7] This appears to be what is requested by the Proposal despite the fact that, as noted in Section I above, a GDPR DPIA is not a suitable vehicle for an assessment of "how the [C]ompany is ensuring appropriate use of, and informed consent for collection of, patient data."

Determinations regarding the Company's legal compliance and business practices require complex analysis, extensive knowledge, and understanding of evolving laws and regulations related to data privacy and healthcare law in multiple jurisdictions across the U.S.; all relevant facts and circumstances about the Company's operations; and industry practice. These matters are multifaceted, complex, and based on factors beyond the expertise of shareholders at large. Thus, a report assessing this aspect of the Company's operations squarely falls within the scope of the traditional ordinary business standard under Rule 14a-8(i)(7). When compounded with the specific requirements of the GDPR DPIA, which is more expansive than the requirements under U.S. law and specifically requires an assessment of various legal compliance matters, including "criminal offence data," "certification scheme[s]," "lawful bas[es] for processing," and "associated compliance and corporate risks,"[8] and as applicable here, would require a determination as to how to apply EU standards to U.S. operations, the Proposal delves even further into ordinary business matters.

While the Proposal makes generic references to oversight of risks and patients' privacy, the underlying subject matter still relates to the Company's policies regarding its legal compliance and how compliance with laws affects the Company's terms of service, which are part of the Company's ordinary day-to-day business operations. *See PayPal* (concurring with the exclusion of a proposal under Rule 14a-8(i)(7) where the company argued that "the [c]ompany's ability to design and oversee its legal compliance program, including the application of the [Acceptable Use Policy], without interference [was] necessary to the operation of the Company's business as a regulated payment services provider"); *JPMorgan Chase & Co. (National Legal and Policy Center)* (avail. Mar. 21, 2023) (concurring with the exclusion of a proposal under Rule 14a-8(i)(7) where the company argued that "[t]he [c]ompany's ability to design and administer its legal compliance program without interference is necessary to the operation of the [c]ompany's business as a regulated financial services company"). Consistent with the cited precedents, the analyses, judgments, and determinations that would be addressed in the report requested by the Proposal therefore are part of the Company's ordinary business operations relating to its legal compliance program, and the Proposal therefore is properly excludable under Rule 14a-8(i)(7).

D. The Proposal Does Not Focus On A Significant Policy Issue That Transcends The Company's Ordinary Business Operations.

The well-established precedents set forth above demonstrate that the Proposal squarely addresses ordinary business matters and, therefore, is excludable under Rule 14a-8(i)(7). The 1998 Release distinguishes proposals pertaining to ordinary business matters from those involving "significant social policy issues." *Id.* (citing Exchange Act Release No. 12999 (Nov. 22, 1976)). While "proposals . . . focusing on sufficiently significant social policy issues (*e.g.*, significant discrimination matters) generally would not be considered to be excludable," the Staff has indicated that proposals relating to both ordinary business matters and significant social

[8] *See* https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

policy issues may be excluded in reliance on Rule 14a-8(i)(7) if they do not "transcend the day-to-day business matters" discussed in the proposals. 1998 Release. In this regard, when assessing proposals under Rule 14a-8(i)(7), the Staff considers "both the proposal and the supporting statement as a whole." Staff Legal Bulletin No. 14C, part D.2 (June 28, 2005). Moreover, as Staff precedents have established, the fact that a proposal may touch upon topics that implicate significant policy issues, or that take such issues as their starting point, does not transform an otherwise ordinary business proposal into one that transcends ordinary business when the proposal does not otherwise focus on those topics.

The Staff most recently discussed how it evaluates whether a proposal "transcends the day-to-day business matters" of a company in Staff Legal Bulletin No. 14L (Nov. 3, 2021) ("SLB 14L"), noting that it is "realign[ing]" its approach to determining whether a proposal relates to ordinary business with the standards the Commission initially articulated in 1976 and reaffirmed in the 1998 Release. In addition, the Staff stated that it will "no longer tak[e] a company-specific approach to evaluating the significance of a policy issue under Rule 14a-8(i)(7)" but rather will consider only "whether the proposal raises issues with a broad societal impact, such that they transcend the ordinary business of the company."

The Staff has consistently concurred with exclusion of proposals that primarily relate to ordinary business matters even if such proposals touch upon significant policy issues. For example, the proposal in *PetSmart, Inc.* (avail. Mar. 24, 2011) requested that the board require its suppliers to certify they had not violated "the Animal Welfare Act, the Lacey Act, or any state law equivalents" which related to preventing animal cruelty. The Staff granted no-action relief under Rule 14a-8(i)(7) because the proposal addressed but did not focus on significant policy issues, stating "[a]lthough the humane treatment of animals is a significant policy issue, we note your view that the scope of the laws covered by the proposal is 'fairly broad in nature from serious violations such as animal abuse to violations of administrative matters such as record keeping.'" Recent precedent where the Staff concurred with exclusion of a proposal that referenced or touched upon a significant policy matter but that addressed or focused on ordinary business matters includes *Fox Corp.* (avail. Sept. 19, 2024). There, the company received a proposal requesting a report on the potential negative social impact and risks to the company from inadequately distinguishing between on-air news content and opinion content, and the company argued that "citing potential social policy implications in a proposal does not qualify as 'focusing' on such issues, even if the social policies happen to be the subject of substantial public focus." The Staff concurred with exclusion under Rule 14a-8(i)(7).

Despite the fact that the Proposal's subject is related to patient data and touches on the issue of privacy, the Proposal does not transcend the Company's ordinary business operations. Rather, as discussed above, the Proposal's principal focus is on the specific terms of service for its AHS businesses, which include how the Company manages patient data, and its legal compliance with data privacy regimes, which is comparable to *PetSmart* and distinguishable from proposals that are directly focused on significant social policy issues. For example, in *Alphabet Inc.* (avail. Apr. 15, 2022), the Staff declined to concur with a request for exclusion under Rule 14a-8(i)(7) where the proposal asked for a report on risks associated with user data collection, privacy, and

security, noting that the proposal transcended ordinary business matters. Unlike the broad social policy issue of data protection in *Alphabet*, here, the Proposal is primarily focused on the narrow ordinary business of the Company's terms of service related to the "appropriate use of, and informed consent for collection of, patient data." In particular, similar to *PetSmart*, the Proposal is focused on requesting a legal compliance assessment based on a DPIA, which requires an assessment of the Company's day-to-day AHS operations and related data processing, rather than an assessment of broad implications related to data protection. In a similar vein, the Proposal is unlike the proposal in *Express Scripts Holding Co.* (avail. Mar. 7, 2018), which requested a review and report on general "cyber risk and actions taken to mitigate that risk." As well, the Proposal is distinguishable from *American Express Co.* (avail. Mar. 6, 2023) and *Laboratory Corp. of America Holdings (Tara Health Foundation)* (avail. Mar. 22, 2023), both addressing proposals that requested a report on the risks and costs of fulfilling information requests regarding customers to aid the enforcement of certain controversial state criminal laws and requesting disclosure of "strategies beyond legal compliance" to minimize or mitigate these risks. There, the proposals focused on the significant social policy issue of specific controversial and recently adopted laws and, in particular, "strategies beyond legal compliance." In contrast, the Proposal is more comparable to *AT&T 2016*, where, as discussed above, the Staff concurred that a proposal focused on its customer account policies—specifically, "a report . . . clarifying the [c]ompany's policies regarding providing information to law enforcement and intelligence agencies, domestically and internationally, above and beyond what is legally required . . . , whether and how the policies have changed since 2013, and assessing risks to the [c]ompany's finances and operations arising from current and past policies and practices" "[did] not focus on a significant policy issue" and was excludable under Rule 14a-8(i)(7) because it related to "procedures for protecting customer information." Accordingly, because the Proposal's subject is the Company's ordinary business operations, the Proposal does not transcend the Company's ordinary business operations and does not focus on any significant policy issue, and therefore the Proposal may be excluded under Rule 14a-8(i)(7).

E. The Proposal May Be Excluded Under Rule 14a-8(i)(7) Because It Seeks To Micromanage The Company.

As explained above, the Commission stated in the 1998 Release that one of the considerations underlying the ordinary business exclusion is "the degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." *Id.* (citing Exchange Act Release No. 12999 (Nov. 22, 1976)). The 1998 Release further states that "[t]his consideration may come into play in a number of circumstances, such as where the proposal involves intricate detail, or seeks to impose specific . . . methods for implementing complex policies." In SLB 14L, the Staff stated that in considering arguments for exclusion based on micromanagement, the Staff "will focus on the level of granularity sought in the proposal and whether and to what extent it inappropriately limits discretion of the board or management." In assessing whether a proposal probes matters "too complex" for shareholders, as a group, to

make an informed judgment, the Staff "may consider the sophistication of investors generally on the matter, the availability of data, and the robustness of public discussion and analysis on the topic." *Id.* The Staff stated that in assessing whether proposals are appropriate for shareholder action, it also would consider "references to well-established national or international frameworks when assessing proposals related to disclosure." *Id.* The Staff's approach "is consistent with the Commission's views on the ordinary business exclusion, which is designed to preserve management's discretion on ordinary business matters but not prevent shareholders from providing high-level direction on large strategic corporate matters." *Id.*

In assessing whether a proposal micromanages by seeking to impose specific methods for implementing complex policies, the Staff evaluates not just the wording of the proposal but also the action called for by the proposal and the manner in which the action called for under a proposal would affect a company's activities and management discretion. *See The Coca-Cola Co.* (avail. Feb. 16, 2022) ("*Coca-Cola 2022*") and *Deere & Co.* (avail. Jan. 3, 2022) (each of which involved a broadly phrased request but required detailed and intrusive actions to implement). *See also Phillips 66* (avail. Mar. 20, 2023) (concurring with the exclusion of a proposal requesting an audited report describing the undiscounted expected value to settle obligations for the company's asset retirement obligations with indeterminate settlement dates, where the no-action request described the extent to which preparation of the report would probe deeply into complex matters); *Valero Energy Corp.* (avail. Mar. 20, 2023) (same). Moreover, "granularity" is only one factor evaluated by the Staff. As stated in SLB 14L, the Staff focuses "on the level of granularity sought in the proposal and whether and to what extent it *inappropriately limits discretion of the board or management*" (emphasis added).

As with the shareholder proposals in *Coca-Cola 2022*, *Deere*, and other precedents discussed below, if the Proposal is indeed interpreted as requiring the Company to follow the referenced DPIA template to assess AHS's treatment of U.S. customer data, the Proposal is excludable under Rule 14a-8(i)(7) because it seeks to micromanage the Company.

1. The Proposal Dictates Specific Methods For How The Company Should Assess And Report On Its Use And Collection Of Patient Data.

Instead of simply allowing shareholders to provide "high-level direction on large strategic corporate matters" or to "suggest targets or timelines" for implementing such matters (as would be appropriate per SLB 14L), the Proposal seeks to impose a specific method for how the Company assesses and discloses its collection and use of U.S. patient data, which would inappropriately limit management's discretion in addressing and implementing the complex issue of managing and disclosing its patient data protection programs and policies.

The approach dictated by the Proposal seeks to micromanage the Company's assessments and disclosures in a way that differs from the methodologies management has determined to adopt to comply with the Company's legal obligations in the jurisdictions in which it operates. In the U.S., the Company is required to comply with federal and state data privacy laws, including those laws that regulate and restrict the collection, use, and disclosure of medical information.

The Company already extensively discloses how it collects, uses, or shares personal data in numerous public explanations including in its privacy notices, which are publicly available and designed to comply with relevant U.S. frameworks, including HIPAA. For example, the Amazon One Medical Notice of HIPAA Privacy Practices describes the typical ways that customers' medical information may be used or disclosed, including for treatment, payment, and healthcare operations, and how customers can get access to their medical information.[9] The Amazon Pharmacy Notice of Privacy Practices contains similar information and also explains that any use or disclosure of a patient's protected health information that is not specifically enumerated in the policy will only be made with the patient's written authorization, which may be revoked in writing at any time.[10] In contrast to these disclosures that operate within the relevant legal framework in the applicable jurisdiction, conducting the Proposal's requested GDPR DPIA would require the Company to set up new systems and processes to assess its data protection policies based on the Proposal's requirements, including altering the way management assesses, tracks, manages, and categorizes the data it collects, uses, stores, and deletes, the nature of its processes, and the measures used to reduce risk, among others. In addition, the Proposal's requested use of the GDPR DPIA to assess the appropriateness of data privacy in the U.S. would require the Company to deviate from the intended purposes of the framework, and apply it outside of both the context and jurisdiction for which it was intended.

The Company's detailed disclosures addressing various federal and state laws demonstrate that the process for assessing and disclosing the Company's patient data policies and procedures is complex, requiring an extensive amount of data collection, research, and ongoing assessment of, and reliance on, established and accepted laws, guidelines, and frameworks. Yet this type of dynamic and multi-faceted process would not be reflected in the GDPR DPIA prescribed in the Proposal.

2. Staff Precedent Supports Exclusion Of The Proposal Under The Micromanagement Standard Of Rule 14a-8(i)(7).

The Proposal eschews management's judgment on the appropriate manner to assess and disclose its patient data policies and procedures and instead seemingly seeks to impose the GDPR DPIA framework in a jurisdiction where it does not apply. The Proposal not only requests an inapposite framework, but the framework is also highly prescriptive, requiring dozens of distinct pieces of information, encompassing thousands of AHS's day-to-day activities. Specifically, the GDPR DPIA template cited and linked to in the Proposal consists of seven steps, each of which is further subdivided into numerous subparts, each of which require detailed assessment and analysis.[11] For example, Step 2 of the GDPR DPIA template consists of the following:

---

[9] *See* https://www.onemedical.com/hipaa/.

[10] *See* https://www.amazon.com/gp/help/customer/display.html?nodeId=GVUKSDLFD49P9GM2.

[11] *See* https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

- A description of the nature of the data processing, including:
  - How the Company will collect data;
  - How the Company will use data;
  - How the Company will store data;
  - How the Company will delete data;
  - The source of the data;
  - Whether the Company will share data with anyone;
  - What types of processing identified as likely high risk are involved; and
  - A flow diagram or other description of data flows;
- A description of the scope of the data processing, including:
  - The nature of the data;
  - Whether the data includes a special category;
  - Whether the data includes criminal offence data;
  - Amount of data that will be collected;
  - Amount of data that will be used;
  - How often the data will be collected;
  - How often the data will be used;
  - How long the data will be kept;
  - How many individuals will be affected; and
  - The geographic areas affected;
- A description of the context of the data processing, including:
  - The nature of the Company's relationship with the individuals;
  - The amount of control the individuals have;
  - Whether the individuals would expect the Company to use the data in a particular way;
  - Whether the individuals affected include children;
  - Whether the individuals affected include vulnerable groups;
  - Whether there were prior concerns over the type of processing;
  - Whether there were prior security flaws;
  - Whether the processing is novel in any way;

  - The current state of technology in the area;
  - Whether there are any current issues of public concern in the area; and
  - Whether the Company has signed up to any approved code of conduct or certification scheme; and
- A description of the purposes of the data processing, including:
  - What the Company aims to achieve;
  - What the intended effects on the individuals are;
  - What the benefits of the processing are for the Company; and
  - What the benefits of the processing are more broadly.

And, this is only one out of seven total steps outlined in the GDPR DPIA template. *See* Exhibit B. The GDPR DPIA is further supplemented by the Guidelines on DPIA,[12] a 22-page document that outlines the principles and assessments required by the GDPR DPIA, and the Guidelines on Data Protection Officers,[13] a 25-page document that, among other things, outlines the role of the data protection officer with respect to a GDPR DPIA. *See* Exhibit C. As such, the Proposal dictates a specific means for assessing and disclosing the Company's patient data protection policies, thereby inappropriately limiting management's discretion as to how to assess the appropriateness of the Company's collection and use of patient data.

In this regard, the Proposal does not provide the Company "high-level direction on large strategic corporate matters" and is not "suggest[ing] targets or timelines." *See* SLB 14L. Instead, the Proposal seeks to restrict management discretion by "impos[ing] a specific method" and "granularity" as to how to the Company is to assess and disclose its patient data policies. *See id.* Moreover, instead of operating within a well-established U.S. disclosure framework, the Proposal's prescriptive approach requires the Company to set up new systems and processes to assess its U.S. operations based on an inapposite EU regulatory framework. The GDPR DPIA was not intended for and does not translate to the U.S. healthcare system, where both the provision of healthcare services (including referrals to other providers) and patients' payment for healthcare services require AHS to share patient data with a complex array of third parties. This is fundamentally different from the approach to healthcare payments in the UK and EU and the framework contemplated by the GDPR. As applied to the Company, the Proposal addresses a complex, multifaceted issue by imposing a prescriptive standard that differs from the approach the Company and U.S. and state lawmakers and regulators believe is best suited to assessing and disclosing patient data privacy matters. The Proposal thus falls clearly within the scope of the 1998 Release and SLB 14L by addressing intricate, granular details and prescribing a specific method for implementing complex policies.

---

[12] *See* https://ec.europa.eu/newsroom/article29/items/611236/en.

[13] *See* https://ec.europa.eu/newsroom/article29/items/612048/en.

Despite the Company's existing disclosures and carefully considered approach to assessment and disclosure of its patient data policies, the Proposal seeks to substitute management's judgment about the appropriate way to address a complex issue. The Proposal is similar to the proposal at issue in *Home Depot, Inc. (Jessica Wrobel)* ("*Home Depot (Wrobel)*") (avail. Mar. 21, 2024), where the proposal requested that the company prepare a living wage report. As with the Proposal, the proponent in *Home Depot (Wrobel)* had cited a reference guide that demonstrated the difficulty in performing living wage calculations. The company characterized the proposal as requiring an unusual and highly prescriptive format for which there was no well-established national or international framework, and that would require assembling granular detail to calculate the requested "living wage" amount and provide specific calculations and statistics based on comparisons of various amounts. The company explained that each element of that process required the collection of data that was not readily available and could be complex. The Staff concurred that the proposal sought to micromanage the company and thereby was excludable under Rule 14a-8(i)(7). *See also Amazon.com, Inc.* (avail. Apr. 1, 2024) (same). *See also Air Products and Chemicals, Inc.* (avail. Nov. 29, 2024), where the proposal requested a detailed report requiring "dozens of distinct pieces of information," prescribing disclosures that "[were] not required by the Commission and [did] not follow any established framework for reporting lobbying activities," and the Staff concurred with exclusion due to micromanagement.

Here, the Proposal is also overly granular and requests specific assessments beyond what the Company has determined to include in its assessments and reports and beyond what is required by any U.S. patient data privacy requirement or framework. The requested assessment would encompass thousands of patients, doctors, clinics, pharmacies, transactions, geographies, products, services, data sources, and operations of the Company, similar to *Home Depot (Wrobel)*. Additionally, given that there is no precedent for using the GDPR DPIA to assess appropriate data use and consent or for reporting based on this EU standard in the U.S., the Company would need to develop and implement new oversight processes for the independent reporting systems that would address gathering, testing, tracking, and assessing those data points. The Proposal's request that the Company oversee an independent GDPR DPIA involves complex and nuanced issues that are not suitable for direct shareholder oversight, and as such, the Proposal is exactly the type that the 1998 Release and SLB 14L recognized as appropriate for exclusion under Rule 14a-8(i)(7).

3. Regardless Of Whether The Proposal Touches Upon A Significant Policy Issue, The Proposal Is Excludable Under Rule 14a-8(i)(7) Because It Seeks To Micromanage The Company.

As discussed above, a proposal may be excluded under Rule 14a-8(i)(7) if it seeks to micromanage a company by specifying in detail the manner in which the company should address an issue, regardless of whether the proposal touches upon a significant policy issue. Here, as discussed in Section II.D, the focus of the Proposal is not on a significant policy issue. Instead, the Proposal is an attempt to direct how the Company addresses the complex and granular issue of patient data privacy as part of AHS's day-to-day operations. But even if the

Proposal were viewed as focused on a significant public policy issue that transcends the Company's ordinary business, it is well established that a proposal that seeks to micromanage a company's business operations is, regardless, excludable under Rule 14a-8(i)(7). *See* Staff Legal Bulletin No. 14E (Oct. 27, 2009) at note 8, citing the 1998 Release for the standard that "a proposal [that raises a significant policy issue] could be excluded under Rule 14a-8(i)(7), however, if it seeks to micro-manage the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Thus, the fact that the Proposal's subject is related to patient data processing matters and touches on the issue of privacy does not preclude its exclusion under Rule 14a-8(i)(7).

CONCLUSION

Based upon the foregoing analysis, the Company intends to exclude the Proposal from its 2025 Proxy Materials, and we respectfully request that the Staff concur that the Proposal may be excluded under Rule 14a-8.

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to shareholderproposals@gibsondunn.com. If we can be of any further assistance in this matter, please do not hesitate to call me at (202) 955-8671, or Mark Hoffman, the Company's Vice President, Associate General Counsel, and Corporate Secretary, at (206) 266-2132.

Sincerely,

Ronald O. Mueller

Enclosures

cc: Mark Hoffman, Amazon.com, Inc.
Lydia Kuykendal, Mercy Investment Services, Inc.
Alexis Fleming, Northwest Women Religious Investment Trust
Eva Horowitz, Miller/Howard Investments, Inc.
Patricia Karr Seabrook, Miller/Howard Investments, Inc.
Nicole Lee, Miller/Howard Investments, Inc.
Father Séamus Finn, Missionary Oblates of Mary Immaculate, US Province
Bernard Voyer, Durocher Fund
Laura Krausa, CommonSpirit Health

EXHIBIT A

RESOLVED, that shareholders of Amazon Inc. ("Amazon") urge the board of directors to oversee an independent Data Protection Impact Assessment[1] on the company's healthcare service offerings that describes how the company is ensuring appropriate use of, and informed consent for collection of, patient data. The assessment should cover Amazon OneMedical and Amazon Pharmacy, be prepared at reasonable cost and omitting confidential and proprietary information and be made available on Amazon's web site.

WHEREAS: In light of publicly[2] discussed problems around the lack of transparency about how Amazon uses data, investors are concerned about the company's plans for protecting a person's most private data - their personal health information. Given the interconnectedness of the company's businesses, we want to know that privacy and data sharing policies are appropriately described and enforced with respect to patient data. A troubling report from NPR implies Amazon is already misleading potential customers into sharing their personal medical information[3].

Americans don't know how companies use their data. One study from Pew Research Center found that 67% say they understand little to nothing about what companies are doing with their personal data, and 73% believe they have little to no control over what companies do with that data[4].

While we expect that Amazon is complying with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant laws, HIPAA only covers certain circumstances with specific and highly sensitive data, and there are privacy concerns that extend beyond its reach. As a regulation, HIPAA focuses on the provider, not the technology solution. This means that privacy risks not protected by HIPAA apply to Amazon, and it is important to know how the company is managing those by informing patients that their data may be used in ways they did not anticipate[5].

In fact, just last year the Federal Trade Commission (FTC) took enforcement action against GoodRx for sharing sensitive personal health information for years with advertising companies and platforms—contrary to its privacy promises—and failed to report these unauthorized disclosures[6]. Of course, Amazon would not need to sell this data in order to monetize it as they own many platforms that use customer data to make a profit, which makes this issue even more concerning. Additionally, last year Senator Josh Hawley wrote a letter to the FTC asking it to investigate the acquisition of OneMedical because of his concerns with Amazon having access to "enormous tranches of patient data"[7].

---

[1] https://gdpr.eu/data-protection-impact-assessment-template/

[2] https://www.washingtonpost.com/technology/2022/07/22/amazon-one-medical-privacy/

[3] https://www.npr.org/2023/05/06/1174468793/amazons-affordable-healthcare-service-has-a-hidden-cost-your-privacy

[4] https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[5] https://www.renalandurologynews.com/features/amazons-virtual-health-clinic-raises-patient-privacy-issues/

[6] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

[7] https://www.techtarget.com/healthtechsecurity/news/366594701/Amazons-Potential-Acquisition-of-One-Medical-Sparks-Health-Data-Privacy-Security-Concerns

We believe that what gets disclosed gets managed. Amazon, a company with a long history of privacy[8] and data protection[9] controversies[10], needs to demonstrate that investors and patients alike can trust it with sensitive data. An assessment that discloses information about how the company is ensuring patients are informed about what data is collected and how it will be used, would mitigate reputational, financial and legal risk from Amazon's commercial healthcare offerings.

[8] https://abcnews.go.com/Technology/collection-voice-data-profit-raises-privacy-fears/story?id=96363792
[9] https://www.reuters.com/technology/look-intimate-details-amazon-knows-about-us-2021-11-19/
[10] https://www.globenewswire.com/news-release/2024/07/16/2913783/0/en/Study-reveals-smart-home-privacy-risks-with-Amazon-Alexa-the-most-hungry-for-user-data.html

EXHIBIT B

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

EXHIBIT C

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248 rev.01

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

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017

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 content

I. Introduction

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA[2]), as does Directive 2016/680[3].

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance**.

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

II. Scope of the Guidelines

[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 (General Data Protection Regulation).

[2] The term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.

[3] Article 27 of the 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, also states that a privacy impact assessment is needed for "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*".

[4] The GDPR does not formally define the concept of a DPIA as such, but

- its minimal content is specified by Article 35(7) as follows:
    - "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
    - *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
    - *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
    - *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*
- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".*

[5] See also recital 84: "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

These Guidelines take account of:

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 218[6];
- the WP29 Guidelines on Data Protection Officer 16/EN WP 243[7];
- the WP29 Opinion on Purpose limitation 13/EN WP 203[8];
- international standards[9].

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by Data Protection Authorities (DPAs) under Article 35(4).

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.

These Guidelines also seek to promote the development of:

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
- a common EU list of processing operations for which a DPIA is not necessary (Article 35(5));
- common criteria on the methodology for carrying out a DPIA (Article 35(5));
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
- recommendations, where possible, building on the experience gained in EU Member States.

[6] WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

III. DPIA: the Regulation explained

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks[10] presented by the processing of personal data.

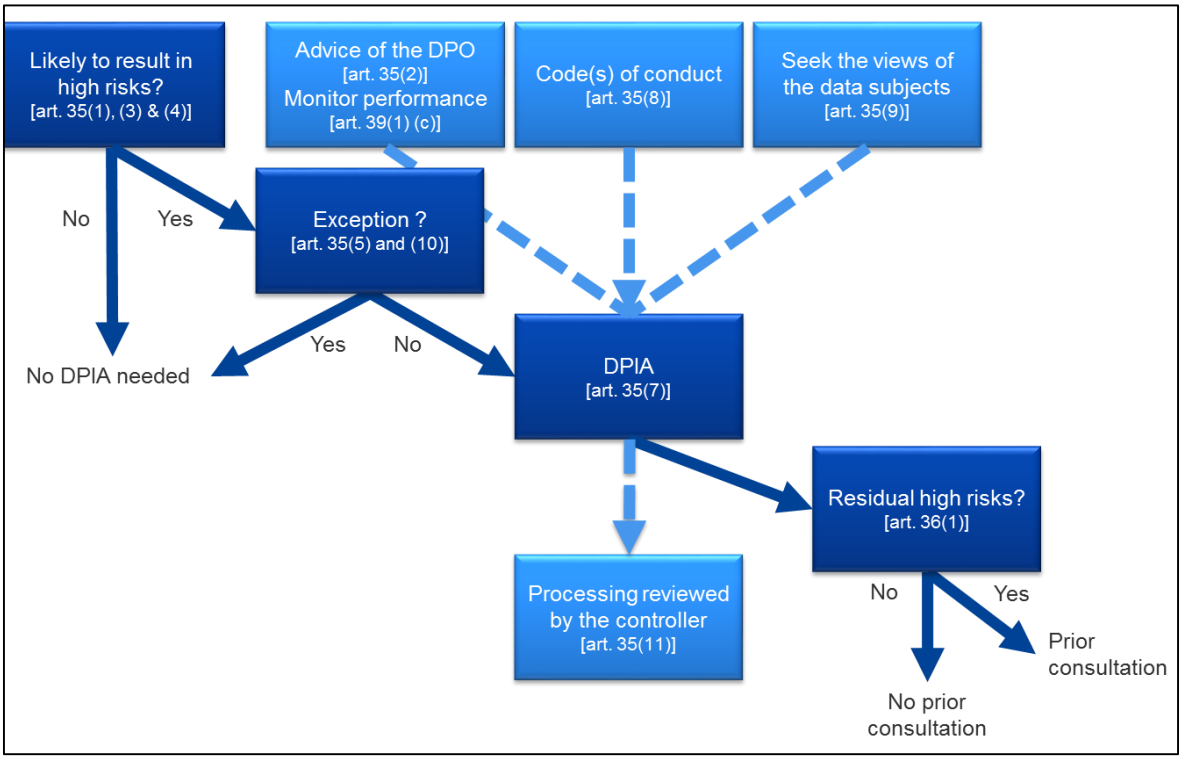
A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".

[10] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.

The following figure illustrates the basic principles related to the DPIA in the GDPR:



A. What does a DPIA address? A single processing operation or a set of similar processing operations.

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks*". Recital 92 adds that "*there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures

designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

B. Which processing operations are subject to a DPIA? Apart from exceptions, where they are "*likely to result in a high risk*".

This section describes when a DPIA is mandatory, and when it is not necessary to carry out a DPIA.

Unless the processing operation meets an exception (III.B.a), a DPIA has to be carried out where a processing operation is "*likely to result in a high risk*" (III.B.b).

a) When is a DPIA mandatory? When processing is "*likely to result in a high risk*".

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[11].

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing operation is "*likely to result in high risks*":

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person[12];*
- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10[13]; or*
- *(c) a systematic monitoring of a publicly accessible area on a large scale*".

[11] See recitals 89, 91 and Article 35(1) and (3) for further examples.

[12] See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".

[13] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processing operations[14], the following nine criteria should be considered.

1. Evaluation or scoring, including profiling and predicting, especially from *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"* (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[15]. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms

[14] See e.g. recitals 75, 76, 92, 116.

[15] The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):

- occurring according to a system;
- pre-arranged, organised or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.

of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale[16]:
    a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
    b. the volume of data and/or the range of different data items being processed;
    c. the duration, or permanence, of the data processing activity;
    d. the geographical extent of the processing activity.
6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject[17].
7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, *etc*.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, *etc*. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

[16] See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

[17] See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

However, in some cases, **a data controller can consider that a processing meeting only one of these criteria requires a DPIA.**

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	**Possible Relevant criteria**	**DPIA likely to be required?**
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects. - Data processed on a large-scale.	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring. - Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, *etc*.	- Systematic monitoring. - Data concerning vulnerable data subjects.	
The gathering of public social media data for generating profiles.	- Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature:	
An institution creating a national level credit rating or fraud database.	- Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature:	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	- Sensitive data. - Data concerning vulnerable data subjects. - Prevents data subjects from exercising a right or using a service or a contract.	

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects.	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- Data processed on a large scale.	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	- Evaluation or scoring.	

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

In addition, as part of the accountability principle, every data controller "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[18]. The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

WP29 considers that a DPIA is not required in the following cases:

- **where the processing is not "*likely to result in a high risk to the rights and freedoms of natural persons*"** (Article 35(1));
- **when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out**. In such cases, results of DPIA for similar processing can be used (Article 35(1)[19]);

[18] In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

[19] "*A single assessment may address a set of similar processing operations that present similar high risks".*

- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed[20] (see III.C);
- **where a processing operation,** pursuant to point (c) or (e) of article 6(1), **has a legal basis** in EU or Member State law, where the law regulates the specific processing operation **and where a DPIA has already been carried out** as part of the establishment of that legal basis (Article 35(10))[21], except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;
- **where the processing is included on the optional list (established by the supervisory authority) of processing operations** for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, *etc*. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with all the relevant requirements of the GDPR.

C. What about already existing processing operations? DPIAs are required in some circumstances.

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

A DPIA is not needed for processing operations that have been checked by a supervisory authority or the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

Conversely, this means that any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations[22], for example because a new technology has come into use or because personal data is

[20] "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

[21] When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities.

[22] In terms of the context, the data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats, *etc*.), security measures and international transfers.

being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned.

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

As a matter of good practice, **a DPIA should be continuously reviewed and regularly re-assessed.** Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

D. How to carry out a DPIA?

a) At what moment should a DPIA be carried out? Prior to the processing.

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93)[23]. This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. **Carrying out a DPIA is a continual process, not a one-time exercise**.

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors.

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

[23] Except when it is an already existing processing that has been prior checked by the Supervisory Authority, in which case the DPIA should be carried out before undergoing significant changes.

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

If the processing is wholly or partly performed by a data processor, **the processor should assist the controller in carrying out the DPIA** and provide any necessary information (in line with Article 28(3)(f)).

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:

- those views could be sought through a variety of means, depending on the context (e.g. a generic study related to the purpose and means of the processing operation, a question to the staff representatives, or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;
- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the DPIA validation process;
- where appropriate, it is recommended to seek the advice from independent experts of different professions[24] (lawyers, IT experts, security experts, sociologists, ethics, *etc*.).
- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f));
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

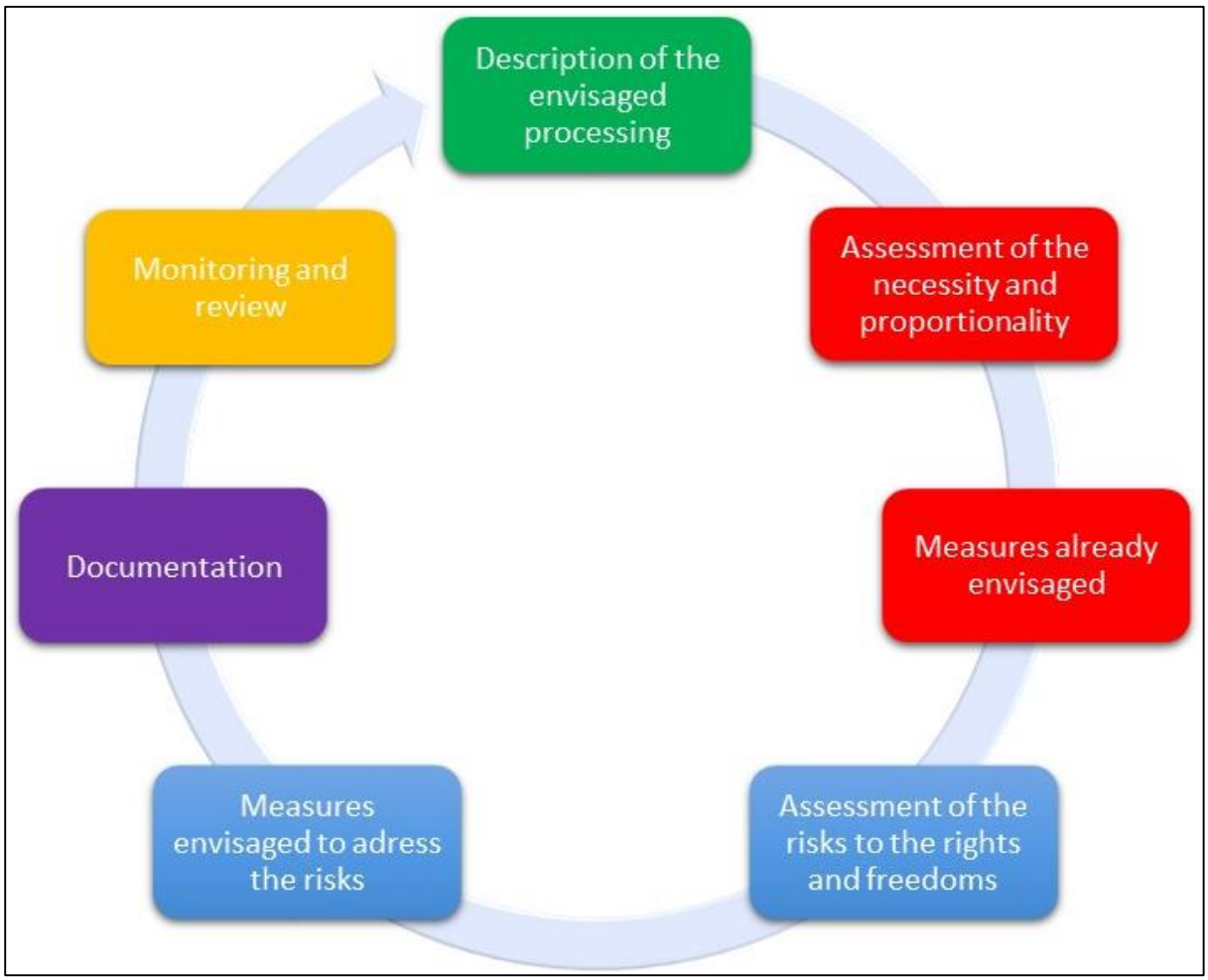
c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "*a description of the envisaged processing operations and the purposes of the processing*";
- "*an assessment of the necessity and proportionality of the processing*";
- "*an assessment of the risks to the rights and freedoms of data subjects*";
- "*the measures envisaged to:*
    - "*address the risks*"*;*
    - "*demonstrate compliance with this Regulation*".

The following figure illustrates the generic iterative process for carrying out a DPIA[25]:



Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.

[25] It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. The DPIA implementation is therefore scalable. This means that even a small data controller can design and implement a DPIA that is suitable for their processing operations.

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well-defined components of risk management (e.g. ISO 31000[26]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following processes, by:

- establishing the context: "*taking into account the nature, scope, context and purposes of the processing and the sources of the risk*";
- assessing the risks: "*assess the particular likelihood and severity of the high risk*";
- treating the risks: "*mitigating that risk*" and "*ensuring the protection of personal data*", and "*demonstrating compliance with this Regulation*".

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security). Conversely, risk management in other fields (e.g. information security) is focused on the organization.

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR. In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. **It is up to the data controller to choose a methodology, but this methodology should be compliant with the criteria provided in Annex 2**.

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.

Finally, where necessary, *"the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation"* (Article 35(11)[27]).

[26] Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.

Moreover, where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice[28], and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents.

E. <u>When shall the supervisory authority be consulted? When the residual risks are high.</u>

As explained above:

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[29] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, *etc*.) in addition to existing policies (notice, consent, right of access, right to object, *etc*.).

In the laptop example above, if the risks have been considered as sufficiently reduced by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) that the data controller must consult the supervisory authority.

[28] Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2).

[29] Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).

An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required[30].

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

IV. Conclusions and recommendations

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.

Where a likely high risk processing is planned, the data controller must:

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:

[30] Note: "*pseudonymization and encryption of personal data*" (as well as data minimization, oversight mechanisms, *etc*.) are not necessarily appropriate measures. They are only examples. Appropriate measures depend on the context and the risks, specific to the processing operations.

    - is compliant with the criteria in Annex 2;
    - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
    - involves the appropriate interested parties and clearly define their responsibilities (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, *etc*.);
- provide the DPIA report to the competent supervisory authority when required to do so;
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;
- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
- document the decisions taken.

Annex 1 – Examples of existing EU DPIA frameworks

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

Examples of EU generic frameworks:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[33] http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[34]).

---

[31] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

[32] See also :

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[34] ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and to data portability (Articles 15 and 20);
      - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
      - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
      - ☐ relationships with processors (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 243 rev.01

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016

As last Revised and Adopted on 5 April 2017

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 content

1 Introduction

The General Data Protection Regulation ('GDPR'),[1] due to come into effect on 25 May 2018, provides a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR.

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO.[2] This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

The concept of DPO is not new. Although Directive 95/46/EC[3] did not require any organisation to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years.

Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.[4] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.

---

[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 (General Data Protection Regulation), (OJ L 119, 4.5.2016). The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement.

[2] The appointment of a DPO is also mandatory for competent authorities under Article 32 of 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 (OJ L 119, 4.5.2016, p. 89–131), and national implementing legislation. While these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[4] See http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

The controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively.

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of these guidelines is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States. The WP29 will monitor the implementation of these guidelines and may complement them with further details as appropriate.

2 Designation of a DPO

2.1. Mandatory designation

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:[5]

a) where the processing is carried out by a public authority or body;[6]
b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data[7] or[8] personal data relating to criminal convictions and offences.[9]

In the following subsections, the WP29 provides guidance with regard to the criteria and terminology used in Article 37(1).

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.[10] This analysis is part of the documentation under the accountability principle. It may be required by the supervisory authority and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services that might fall within the cases listed in Article 37(1).

When an organisation designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory.

---

[5] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well.

[6] Except for courts acting in their judicial capacity. See Article 32 of Directive (EU) 2016/680.

[7] Pursuant to Article 9 these include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[8] Article 37(1)(c) uses the word '*and*'. See Section 2.1.5 below for explanation on the use of '*or*' instead of '*and*.'

[9] Article 10.

[10] See Article 24(1).

Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data. In this case it is important to ensure that there is no confusion regarding their title, status, position and tasks. Therefore, it should be made clear, in any communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a data protection officer (DPO). [11]

The DPO, whether mandatory or voluntary, is designated for all the processing operations carried out by the controller or the processor.

2.1.1 'PUBLIC AUTHORITY OR BODY'

The GDPR does not define what constitutes a '*public authority or body'*. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[12] In such cases, the designation of a DPO is mandatory.

A public task may be carried out, and public authority may be exercised[13] not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO. Such a DPO's activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

[11] This is also relevant for chief privacy officers ('CPO's) or other privacy professionals already in place today in some companies, who may not always meet the GDPR criteria, for instance, in terms of available resources or guarantees for independence, and, if they do not, they cannot be considered and referred to as DPOs.

[12] See, e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, p. 90).

[13] Article 6(1)(e).

2.1.2 'CORE ACTIVITIES'

Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor'*. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.

However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.

As another example, a private security company carries out the surveillance of a number of private shopping centres and public spaces. Surveillance is the core activity of the company, which in turn is inextricably linked to the processing of personal data. Therefore, this company must also designate a DPO.

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

2.1.3 'LARGE SCALE'

Article 37(1)(b) and (c) requires that the processing of personal data be carried out on a large scale in order for the designation of a DPO to be triggered. The GDPR does not define what constitutes large-scale processing, though recital 91 provides some guidance.[14]

Indeed, it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop for identifying in more specific and/or quantitative terms what constitutes '*large scale*' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.

In any event, the WP29 recommends that the following factors, in particular, be considered when

[14] According to the recital, '*large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk*' would be included, in particular. On the other hand, the recital specifically provides that '*the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer'*. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus processing of data of a whole country or across Europe); there is a large grey zone in between these extremes. In addition, it should be borne in mind that this recital refers to data protection impact assessments. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.

determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

2.1.4 'REGULAR AND SYSTEMATIC MONITORING'

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but the concept of '*monitoring of the behaviour of data subjects*' is mentioned in recital 24[15] and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.

However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.[16]

WP29 interprets 'regular' as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times

[15] *'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.*

[16] Note that Recital 24 focuses on the extra-territorial application of the GDPR. In addition, there is also a difference between the wording '*monitoring of their behaviour'* (Article 3(2)(b)) and *'regular and systematic monitoring of data subjects'* (Article 37(1)(b)) which could therefore be seen as constituting a different notion.

- Constantly or periodically taking place

WP29 interprets 'systematic' as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

2.1.5 SPECIAL CATEGORIES OF DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

Article 37(1)(c) addresses the processing of special categories of data pursuant to Article 9, and personal data relating to criminal convictions and offences set out in in Article 10. Although the provision uses the word 'and', there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say 'or'.

2.2. DPO of the processor

Article 37 applies to both controllers[17] and processors[18] with respect to the designation of a DPO. Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).

It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.

Examples:

- A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out

[17] The controller is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.

[18] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.

large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

- A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

The DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

2.3. Designation of a single DPO for several organisations

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects[19], the supervisory authority[20] but also internally within the organisation, considering that one of the tasks of the DPO is *'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this Regulation'*.[21]

In order to ensure that the DPO, whether internal or external, is accessible it is important to make sure that their contact details are available in accordance with the requirements of the GDPR.[22]

He or she, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects[23] and cooperate[24] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

According to Article 37(3), a single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

---

[19] Article 38(4): '*data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation*'.

[20] Article 39(1)(e): '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult, where appropriate, with regard to any other matter*'.

[21] Article 39(1)(a).

[22] See also Section 2.6 below.

[23] Article 12(1): *'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'*

[24] Article 39(1)(d) *: 'to cooperate with the supervisory authority'*

2.4. Accessibility and localisation of the DPO

According to Section 4 of the GDPR, the accessibility of the DPO should be effective.

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union.

However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union[25], a DPO may be able to carry out his or her activities more effectively if located outside the EU.

2.5. Expertise and skills of the DPO

Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'. Recital 97 provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

- **Level of expertise**

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.

- **Professional qualities**

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

[25] See Article 3 of the GDPR on the territorial scope.

- **Ability to fulfil its tasks**

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing[26], data subjects' rights[27], data protection by design and by default[28], records of processing activities[29], security of processing[30], and notification and communication of data breaches.[31]

- **DPO on the basis of a service contract**

The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that each member of the organisation exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.

2.6. Publication and communication of the DPO's contact details

Article 37(7) of the GDPR requires the controller or the processor:

- to publish the contact details of the DPO and
- to communicate the contact details of the DPO to the relevant supervisory authorities.

The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) and the supervisory authorities can easily and directly contact the DPO without having to contact another part of the organisation. Confidentiality is equally important: for example, employees may be reluctant to complain to the DPO if the confidentiality of their communications is not guaranteed.
The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)).

[26] Chapter II.
[27] Chapter III.
[28] Article 25.
[29] Article 30.
[30] Article 32.
[31] Articles 33 and 34.

The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.[32]

However, communication of the name of the DPO to the supervisory authority is essential in order for the DPO to serve as contact point between the organisation and the supervisory authority (Article 39(1)(e).

As a matter of good practice, the WP29 also recommends that an organisation informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.

3 Position of the DPO

3.1. Involvement of the DPO in all issues relating to the protection of personal data

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is *'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'*.

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.[33] Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.

Consequently, the organisation should ensure, for example, that:

- The DPO is invited to participate regularly in meetings of senior and middle management.

[32] It is notable that Article 33(3)(b), which describes information that must be provided to the supervisory authority and to the data subjects in case of a personal data breach, unlike Article 37(7), specifically also requires the name (and not only the contact details) of the DPO to be communicated.
[33] Article 35(2).

- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
- The DPO must be promptly consulted once a data breach or another incident has occurred.

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.

3.2. Necessary resources

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.* The following items, in particular, are to be considered:

- Active support of the DPO's function by senior management (such as at board level).
- Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.

3.3. Instructions and '*performing their duties and tasks in an independent manner*'

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO '*does not receive any instructions regarding the exercise of [his or her] tasks.*' Recital 97 adds that DPOs, '*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*'.

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.[34] If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO '*shall directly report to the highest management level of the controller or the processor'*. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.

3.4. Dismissal or penalty for performing DPO tasks

Article 38(3) requires that DPOs should *'not be dismissed or penalised by the controller or the processor for performing [their] tasks'*.

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.

[34] Article 5(2).

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

3.5. Conflict of interests

Article 38(6) allows DPOs to '*fulfil other tasks and duties'*. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests'*.

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:

- to identify the positions which would be incompatible with the function of DPO
- to draw up internal rules to this effect in order to avoid conflicts of interests
- to include a more general explanation about conflicts of interests
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally

4 Tasks of the DPO

4.1. Monitoring compliance with the GDPR

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO '*should assist the controller or the processor to monitor internal compliance with this Regulation*'.

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities
- analyse and check the compliance of processing activities
- inform, advise and issue recommendations to the controller or the processor

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

4.2. Role of the DPO in a data protection impact assessment

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice'* of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35*'.

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others [35]:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account[36].

[35] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have '*at least'* the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail.

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.

4.3. Cooperating with the supervisory authority and acting as a contact point

According to Article 39(1)(d) and (e), the DPO should '*cooperate with the supervisory authority*' and '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter'*.

These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

4.4. Risk-based approach

Article 39(2) requires that the DPO '*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*'.

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

[36] Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure **and to be able to demonstrate** that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'.

4.5. Role of the DPO in record-keeping

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to '*maintain a record of processing operations under its responsibility*' or *'maintain a record of all categories of processing activities carried out on behalf of a controller'*.

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[37]

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.

[37] Article 24(1)(d), Regulation (EC) 45/2001.

5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the General Data Protection Regulation (GDPR) to appoint a DPO.

Designation of the DPO

1 Which organisations must appoint a DPO?

The designation of a DPO is an obligation:

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
- if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
- if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

Note that Union or Member State law may require the designation of DPOs in other situations as well. Finally, even if the designation of a DPO is not mandatory, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts. When an organisation designates a DPO on a voluntary basis, the same requirements will apply to his or her designation, position and tasks as if the designation had been mandatory.

Source: Article 37(1) of the GDPR

2 What does 'core activities' mean?

'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.

On the other hand, all organisations carry out certain supporting activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

Source: Article 37(1)(b) and (c) of the GDPR

3 What does 'large scale' mean?

The GDPR does not define what constitutes large-scale processing. The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- the geographical extent of the processing activity

Examples of large scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

Source: Article 37(1)(b) and (c) of the GDPR

4 What does 'regular and systematic monitoring' mean?

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

WP29 interprets 'regular' as meaning one or more of the following:

- ongoing or occurring at particular intervals for a particular period
- recurring or repeated at fixed times
- constantly or periodically taking place

WP29 interprets 'systematic' as meaning one or more of the following:

- occurring according to a system

- pre-arranged, organised or methodical
- taking place as part of a general plan for data collection
- carried out as part of a strategy

Source: Article 37(1)(b) of the GDPR

5 Can organisations appoint a DPO jointly? If so, under what conditions?

Yes. A group of undertakings may designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation. In order to ensure that the DPO is accessible, whether internal or external, it is important to make sure that their contact details are available. The DPO, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

A single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

Source: Article 37(2) and (3) of the GDPR

6 Where should the DPO be located?

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union. However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.

7 Is it possible to appoint an external DPO?

Yes. The DPO may be a staff member of the controller or the processor (internal DPO) or fulfil the tasks on the basis of a service contract. This means that the DPO can be external, and in this case, his/her function can be exercised based on a service contract concluded with an individual or an organisation.

When the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable requirements of the GDPR.

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, the Guidelines recommend to have, in the service contract, a clear allocation of tasks within the external DPO team and to assign a single individual as a lead contact and person 'in charge' of the client.

Source: Article 37(6) of the GDPR

8 What are the professional qualities that the DPO should have?

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his or her tasks.

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

Relevant skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- understanding of the processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- ability to promote a data protection culture within the organisation

Source: Article 37(5) of the GDPR

Position of the DPO

9 What resources should be provided to the DPO by the controller or the processor?

The DPO must have the resources necessary to be able to carry out his or her tasks.

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- active support of the DPO's function by senior management
- sufficient time for DPOs to fulfil their tasks
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- official communication of the designation of the DPO to all staff
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- continuous training

Source: Article 38(2) of the GDPR

10 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner? What does 'conflict of interests' mean?

Several safeguards exist in order to enable the DPO to act in an independent manner:

- no instructions by the controllers or the processors regarding the exercise of the DPO's tasks
- no dismissal or penalty by the controller for the performance of the DPO's tasks
- no conflict of interest with possible other tasks and duties

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Source: Article 38(3) and 38(6) of the GDPR

Tasks of the DPO

11 What does 'monitoring compliance' mean?

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities
- analyse and check the compliance of processing activities
- inform, advise and issue recommendations to the controller or the processor

Source: Article 39(1)(b) of the GDPR

12 Is the DPO personally responsible for non-compliance with data protection requirements?

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and to be able to demonstrate that processing

is performed in accordance with this Regulation. Data protection compliance is the responsibility of the controller or the processor.

13 What is the role of the DPO with respect to data protection impact assessments and records of processing activities?

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

Source: Article 39(1)(c) and Article 30 of the GDPR

Done in Brussels, on 13 December 2016

For the Working Party,
The Chairwoman

Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

For the Working Party
The Chairwoman

Isabelle FALQUE-PIERROTIN