LEWIS SILKIN

# Article 29 Working Party's Guidelines on GDPR

ARTICLE 29 WORKING PARTY'S GUIDELINES ON GDPR

The Article 29 Working Party (**WP29**), an advisory body made up of a representative from the data protection authority of each EU Member State, and includes the European Data Protection Supervisor and the European Commission, has provided helpful guidelines in relation to the GDPR. Although, its opinions and guidelines are not binding, they shed a welcome light and help interpret some of the principle based GDPR requirements.

On 13 December 2016, the Article 29 Working Party (WP29) published guidelines together with FAQs on three key areas of GDPR. These include:

- The right to data portability
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf
- Data Protection Officers (DPOs)
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf
- Lead Supervisory Authority
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_annexii_en_40858.pdf

On 4 April 2017 the WP29 published Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR. These Guidelines were subsequently updated on 4 October 2017.

http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

We set out below a summary of the key points for each guideline.

### 1. The right to data portability

The GDPR introduces a brand new right to data portability and compliance will require organisations to make operational changes to their systems and databases in order to comply. The WP29 guidelines on the right to data portability provide guidance on the interpretation and the implementation of the new right to data portability. It aims at defining its scope and the conditions under which it applies irrespective of the legal basis of the data processing. The WP29 also recommends that data controllers and generally industry stakeholders and trade associations work together towards the creation of systems and tools as well as interoperable standards and formats so as to facilitate the response to data portability requests.

| Key issue | Changes introduced by GDPR |
|---|---|
| **Definition** | Data subjects have the right to enjoy more control over their personal data, especially to reuse and manage it, or to switch between service providers.<br>They "have the right (i) to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly-used and machine-readable format and have the right (ii) to transmit those data to another controller without hindrance from the controller to which the data have been provided…" |
| **Legal basis** | There is no general right of data portability.<br>It only applies to data being processed with the data subject's consent or pursuant to the necessity to perform a contract.<br>Other legal bases, such as processing that is required by law, or for the legitimate interest of the controller do not apply. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Interaction with Data Subject Access requests** | Data portability is expected to complement the existing data access subject rights which will remain available to individuals. |
| **Scope of the data** | Data portability only applies to data processed by automated means and therefore excludes paper files.<br><br>**In scope:** only personal data which concerns the data subject. It includes both the data provided by individuals and the personal data generated by a data subject's activity, including:<br>• through the use of the controller's services or device (such as data search history, traffic data, browsing behaviour or location data)<br>• pseudonymous data clearly relating to a data subject; and<br>• personal data relating to several other data subjects<br><br>**Out of scope:** data inferred or derived by the data controller on the basis of the personal data provided by the data subject. Example: user profile or algorithmic results based on the data collected, credit score or analysis of the user's health.<br><br>**Limitations:** which cannot "in and of itself serve as the basis for a refusal to answer the portability request" include:<br>• the prohibition to transmit data which may adversely affect the rights and freedoms of a third party, unless the receiving data controller is pursuing a legitimate interest<br>• restrictions related to applicable trade secrets and intellectual property rights, such as database rights |
| **Format of the data** | The many types of data that data subjects may request make it difficult to identify one format and it is recognised that there is no one appropriate format for providing this data, as long as it is "interoperable" for ease of sharing with other controllers.<br><br>**Minimum standards** for the provision of the data by data controllers include:<br>• to provide for a high level of abstraction to allow for the data controller to remove information which is outside the scope of portability, such as passwords<br>• to provide as much metadata as possible in order to preserve the precise meaning of the exchanged information; and<br>• to securely deliver information to the correct individual and ensure that the information is transmitted and stored as securely as possible |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Specific technical obligations for Data Controllers** | Data controllers are required to provide a range of tools and technical measures to facilitate data subject's requests including the provision of:<br>• a process for acknowledging receipt of requests, to confirm the identity of the data subject and respond to the requests without undue delay<br>• a direct download option from the controller's website and an option to automatically transmit data to another data controller. Example: providing an application programming interface (API) may help |
| **General obligations for Data Controllers** | • **Inform** data subjects regarding the availability of the new right to portability "in a concise, transparent, intelligible, and easily accessible form, using clear and plain language" (including before any account closure)<br>• **Respond** to requests without undue delay, and in any event within one month of the initial request<br>• **Identify** and implement an authentication procedure so as to verify the identity of the data subject exercising the request. Should the identity of a data subject raise doubts, further information may be requested to confirm the data subject's identity before complying with the request<br>• **Time** extension in the event that the data requested may prove difficult to transfer, for up to three months from the relevant supervisory authority<br>• **Fees** for the service may not be charged unless the request can be shown to be "manifestly unfounded or excessive", but this only may be permitted in exceptional cases<br>• **Implement all security** and authentication measures necessary to ensure the secure transmission and storage of the personal data of data subjects (e.g., by use of encryption) to the right destination (e.g., by use of additional authentication information). Because of the risk that data subjects might request for their data but then fail to keep it secure, controllers responding to portability requests should recommend appropriate format(s) and encryption measures to help the data subject maintain security<br>• **Interoperability** so that personal data may be accessed by most other data controllers in a common format |
| **Interaction with Data Retention and Erasure** | Data portability does not impact data retention obligations. Organisations are not required to retain personal data in the event that a data subject may choose to exercise this right. Similarly, a data subject's data portability request does translate by itself into a request to delete that data subject's personal data. Data retention and Data portability requirements apply in parallel. |

## 2. Data Protection Officers

Although the role of DPOs is already required by some Member States' national laws (such as Germany and Sweden), it is not currently mandatory under EU Data Protection Law, to appoint a DPO. The GDPR will introduce significant new obligations which will require many organisations to appoint DPOs. The WP29 recognise the importance of DPOs as being "at the heart" and at the forefront of the organisation's obligation to comply with the requirements of the GDPR. The new guidelines on DPOs provide businesses with useful information on the roles and responsibilities of DPOs.

| Key issue | Changes introduced by GDPR |
|---|---|
| **Definition** | A DPO is a person (either an employee or an external consultant) who is given formal responsibility for data protection compliance within an organisation. |
| **Legal basis** | Article 37(1) of the GDPR requires the mandatory designation of a DPO in the following three cases:<br>• the relevant data processing activity is carried out by a public authority or body<br>• the data controller or processor's core activities involve regular and systematic monitoring of data subjects, on a large scale; or<br>• the data controller or processor's core activities of the relevant business involve processing of special categories of data, or data relating to criminal convictions and offences, on a large scale<br>The guidelines provide a more detailed explanation of these concepts, enabling businesses to better understand their compliance obligations. |
| **Rules on DPO's appointment** | The guidelines clarify key concepts used in the GDPR:<br>• **Core activities** are described as those activities that "can be considered as the key operations necessary to achieve the controller's or processor's goals". Conversely, "core activity" may not include standard IT support or employee compensation which should be considered "ancillary functions" rather than a company's "core activity"<br>• **Large scale** of special categories of personal data (referred in many cases as "sensitive data") consists of "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"<br>Such qualification may depend on a number of factors including:<br>– the number of data subjects concerned, either as a specific number or as a proportion of the relevant population<br>– the volume of data and/or the range of different data items being processed<br>– the duration, or permanence, of the data processing activity<br>– the geographical extent of the processing activity<br>Examples of "large scale" sensitive data processing include hospital's processing of patient data, whereas examples of "non-large scale" processing include an individual lawyer's processing of criminal convictions. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Rules on DPO's appointment (continued)** | • **Regular and Systematic Monitoring** include "all forms of profiling and tracking on the internet, including for purposes of behavioural advertising". Clearly, behavioural advertising agencies will be required to appoint a DPO. Other examples include: the operation of a telecommunications network; profiling and scoring for the purposes of risk assessment; location tracking; fitness and health data via wearable devices; and connected devices<br><br>Organisations are required to carry out an internal analysis so as to determine whether they require a DPO. It is left to the discretionary decision of the organisations that may not require a DPO to designate a DPO on a voluntary basis. In such case, all GDPR requirements on DPO's position and tasks shall become mandatory.<br><br>However, they may also appoint other staff to perform tasks relating to data protection compliance. It is important for such staff not to be referred as "DPOs" so as to or avoid any amalgamation with the status of a DPO appointed voluntarily. |
| **DPO requirements** | The requirements that designated DPOs are expected to fulfil are as follows:<br>• **Accessibility** – a group of undertakings can appoint a single DPO, as long as he or she is personally available to efficiently communicate with data subjects, supervisory authorities and internally within the organisation (including in the language or languages of the supervisory authorities or data subjects concerned). A single DPO must be able to perform their tasks efficiently despite being responsible for several undertakings<br>• **Expertise** - the DPO must have a level of expertise that is commensurate to the sensitivity, complexity and amount of data processed by the relevant organisation (i.e. importance of the transfers outside EEA)<br>A DPO can be appointed on a part-time basis, alongside other duties, provided that those other duties do not give rise to conflicts of interest and as long as the DPO is given sufficient time to fulfil their duties as a DPO.<br><br>An external DPO, or DPO team may be appointed, provided that the DPO must be able to fulfil its / their tasks, they must be independent and they must be afforded sufficient protection (for example, from unfair termination of a service contract).<br>• **Professional qualities** - the DPO should have expertise in national and European data protection law, including an in-depth knowledge of the GDPR. DPOs appointed for public authorities should have an excellent knowledge of the administrative procedures of their organisation, while DPOs operating in the private sector must also have a good knowledge of the industry within which they are active<br>• **Ability to fulfil task** - the DPO should demonstrate integrity and high professional ethics and, as a primary concern, enable compliance with the GDPR |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Role of the DPO** | Organisations are required to seek and consider the DPO's advice at all times and from the earliest stage possible, on all issues relating to the protection of personal data.<br><br>As part of the organisations' standard governance rules, the DPO will need to be appropriately informed on all relevant associated matters; invited to participate regularly in meetings of senior and middle management; and required to attend whenever projects have data protection implications; and promptly consulted once a data breach or other incident has occurred.<br><br>DPOs' tasks may include:<br>• monitoring the organisation's compliance with the GDPR, and advising on data protection issues<br>• carrying out data protection impact assessments. Where high-risk processing is contemplated, the business should actively seek advice from the DPO on conducting a DPIA. The DPO is expected to take a risk-based approach, and prioritising the assessment of high-risk processing activities; and<br>• other data protection related tasks such as maintaining the record of processing operations |
| **Protection for DPOs** | In order to protect DPO's autonomous and independent status within an organisation, they benefit from protections against unfair dismissal or termination based on the performance of their role. In some EU Member States, a DPO who has the status of an employee may also benefit from the protections afforded by local employment law. In case of disagreement with the DPO, the organisation will need to document its reasons why the DPO's advice is not being followed. Due to the high level of responsibilities given to DPOs, they cannot be terminated or otherwise penalised (e.g. demotion, denial of promotion, etc.) for providing advice within the scope of their responsibilities albeit contrary to the organisation's view. The same protections apply should an organisation decide to appoint an external DPO (e.g., no unfair termination of the service contract for activities as DPO). |

### 3. Lead Supervisory Authority

The WP29 provides guidelines for identifying a controller or processor's lead supervisory authority. This set of guidelines is especially helpful for those companies that carry out cross-border processing of personal data, defined as data processing that takes place when a controller or processor has establishments in multiple Member States, or where the controller or processor is established in a single Member State but the processing "substantially affects or is likely to substantially affect" data subjects in multiple Member States. These rules will determine which DPA takes the lead in any enforcement action with a cross border dimension. These GDPR rules aim to simplify and improve the relationship of multinational organisations established in various Member States with the relevant DPAs as opposed to being subject to multiple DPAs in each jurisdiction.

This set of guidelines recognizes that the designation of a lead supervisory authority necessarily is a very fact-specific inquiry. Although it provides some generalized advice, it also includes illustrative examples and factors for companies to consider in making the determination for themselves. To that end, the guidelines also include an annex meant to guide companies going through the designation process. Some of the more general points are described below.

In these situations, the GDPR allows controllers and processors to designate a single local authority to act as the "lead supervisory authority" which role is to oversee their operations and compliance with the law. This has become known as the "one stop shop" approach.

| Key issue | Changes introduced by GDPR |
|---|---|
| **The "one-stop shop mechanism"** | This is one of the central pillars of the GDPR. It is also called "consistency mechanism". It is meant to help multinational organisations deal with a single supervisory authority, in spite of having a number of establishments across the EU Member States.<br><br>This mechanism is available to both controllers and processors carrying out the "cross-border processing" of personal data in the event that either may have:<br>• establishments in two or more EU Member States and the processing of personal data takes place in the context of their activities in those establishments; or<br>• only carries out data processing activities in the context of its establishment in one EU Member State, but the activity substantially affects, or is likely to substantially affect data subjects in more than one EU Member State |
| **Identifying the Lead Supervisory Authority** | The designation of a lead supervisory authority is driven by very fact-specific parameters.<br><br>For **controllers** engaged in cross-border data processing, the lead supervisory authority will be the supervisory authority in the Member State in which the controller has its "main establishment" or "single establishment". The definition of the main establishment refers to the place of the "central administration" of the controller in the EU and where the controller makes "decisions on the purposes and means of the processing". However, if data protection decision-making occurs in different EU Member States, several detailed examples explain how to determine in which EU jurisdiction is the "main establishment".<br><br>For **processors** with establishments in more than one EU Member State, they may also benefit from the "one-stop-shop mechanism". The processor's main establishment will be the place of the central administration of the processor in the EU or, if there is no central administration in the EU, the establishment in the EU where the main processing takes place. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Identifying the Lead Supervisory Authority (continued)** | For **Groups of undertakings**, the lead authority is likely to be the authority in the Member State where the undertaking with overall control is established – this is likely to be the parent undertaking or "central administration".<br><br>Where groups of companies have more complex decision-making processes, with different establishments having independent decision-making powers, the lead authority will be in the Member State where the exercise of management activities that determine the main decisions relating to personal data takes place.<br><br>In cases involving both controller and processor, the competent lead supervisory authority will be the lead supervisory authority for the controller. |
| **Role of the Lead Supervisory Authority** | The lead supervisory authority will have primary responsibility for dealing with cross-border processing activities and will coordinate investigations into breaches by the controller or processor. |
| **Companies not established in the EU** | The one-stop shop system is not available to an organisation which does not have any establishment in the EU. Such organisation will be subject to the supervisory authorities in each EU Member State in which it operates. The fact that an organisation may have appointed a single representative in one Member State does not mean that person may qualify as a "main establishment" for one-stop shop purposes. This requirement may weigh in heavily on SMEs. |
| **Prohibition of "Forum Shopping"** | Controller and processors are not allowed to do any 'forum shopping' choosing a supervisory authority by claiming they have their main establishment in such Member State when the management activity is actually exercised in another Member State. Supervisory authorities may challenge the designation by an organisation of a lead authority and ultimately decision may be referred to the European Data Protection Board (EDPB) to objectively define which authority is in fact the "lead". |
| **Concerned authorities** | When the one-stop-shop mechanism is available, the lead supervisory authority will closely involve and co-ordinate other "concerned" authorities in its enforcement of the GDPR.<br><br>Lead authorities must consult with "concerned" supervisory authorities through the cooperation procedures set out in the GDPR. A supervisory authority may be "concerned":<br>• if the controller or processor has an establishment in that Member State, and<br>• if data subjects residing in that Member State will be substantially affected by processing, or<br>• if a complaint has been lodged with that Member State<br><br>Concerned authorities will therefore have competence to oversee how a case is dealt with when either of these criteria apply. A lead authority may decide not to handle a case if it would be more appropriate for the concerned supervisory authority who informed the lead authority of the case to do so. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **Data subject's rights** | Data subjects may lodge a complaint with any supervisory authority. However, such supervisory authority will then be required to inform the lead supervisory authority, which will in turn determine whether it will handle the complaint. If the lead supervisory authority decides that it does not have "jurisdiction" to handle the complaint itself, the supervisory authority to whom the complaint was made will handle it. |
| **The European Data Protection Board ("EDPB")** | The European Data Protection Board ("EDPB") is a body established under the GDPR, which will succeed to the WP29.<br><br>Likewise, it will include the head or representative of one supervisory authority from each Member State and of the European Data Protection Supervisor ("EDPS"). The European Commission also has a non-voting right to participate on the Board. The EDPB has a lengthy list of tasks. Whereas the WP29, was essentially an advisory committee producing recommendations and opinions, the EDPB will have a more formal and binding role relating to the enforcement of data protection law. The primary obligation of the EDPB is to ensure the consistent application of the GDPR by the EU Member States. |

### 4. Data Protection Impact Assessment

Article 35 of the GDPR introduces the concept of DPIAs. This is a process designed to manage the risks of data processing and assist data controllers in complying with their obligations under the GDPR. DPIAs help controllers to focus on the specific processes they are adopting and consider whether they are necessary and proportionate.

Article 35(1) of the GDPR states that DPIAs are required when the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons". The relevant "rights and freedoms" include the right to data protection and privacy, as well as rights such as the right of freedom of speech and the prohibition of discrimination.

Although it is not mandatory to carry out a DPIA, if a supervisory authority concludes that an assessment should have been carried out (and has not been carried out) a data controller could be hit with the higher of 1) a fine of up to 10 million Euros or 2) in the case of an undertaking, up to 2% of the total worldwide annual turnover the company.

| Key issue | Changes introduced by GDPR |
|---|---|
| **Who should carry out a DPIA?** | Data controllers are responsible for carrying out DPIAs. Data processors and data processing officers (if relevant) should also assist.<br><br>Data subjects should be consulted where appropriate. Where data subjects are consulted and the data controller goes against the view of the data subject, the controller's justification for continuing processing the data should be documented. |
| **What does a DPIA address?** | A DPIA can address a single processing operation or multiple operations which are similar in terms of their nature, scope, context, purpose and risk.<br><br>If there is more than one controller, each respective controller should set out clearly their own obligations. |
| **When is a DPIA mandatory?** | A DPIA is mandatory when processing is *"likely to result in a high risk to the rights and freedoms of natural persons".*<br><br>The carrying out of an assessment is particularly important when a new data processing technology is being used.<br><br>The GDPR provides a non-exhaustive list of examples where processing is "likely to result in high risks" these include:<br>• **systematic and extensive evaluation** based on **automated processing**, including profiling, where this processing leads to decisions which will **legally or otherwise significantly affect** an individual<br>• processing a large amount of **highly sensitive data** (including data on criminal convictions)<br>• **systematic monitoring** of a public area on a **large scale** |
| **What is "systematic and extensive evaluation?"** | This will include profiling and predicting, particularly if the controller is considering the data subject's performance at work, economic situation, health, interests, location or movements. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **What is "automated processing" which has a "legal" or otherwise significant effect?** | In this instance the data controller will be processing data for the purpose of making a decision which will have a legal or similar effect on a person. For example, processing may be carried out to exclude or discriminate against a data subject. |
| **What does "highly sensitive personal data" include?** | This includes a data subject's political opinion, medical health and information relating to criminal convictions. For example, DPIA will be necessary where hospitals retain sickness records, or where location data and financial data is collected. |
| **What is "systematic monitoring" in a public area?** | This is data collected through a network.<br>This is taken particularly seriously as data subjects might not know that they are being monitored. |
| **What is considered a "large scale"?** | This is not defined within the GDPR but controllers should consider the number of data subjects, the volume of data, the geographical extent of processing and the length of time that data is intended to be held. |
| **What other factors would indicate that a DPIA should be carried out?** | • Matching data from two or more separate processing activities<br>• Processing data of vulnerable data subjects (for example individuals who are mentally ill or elderly, asylum seekers and medical patients)<br>• When processing would prevent a data subject from exercising a right or using a service, for example, when banks carry out credit screening |
| **In which circumstances should a DPIA be carried out?** | Where data processing meets two of the six bullet points above, it is more likely that processing will involve a "high risk to rights and freedoms of natural persons". In these cases, a DPIA should be carried out.<br>Having said this, there may be instances where two factors are present and controllers consider that carrying out a DPIA is not necessary. In these circumstances, controllers should document their reasoning.<br>In other cases, DPIAs may be required when only one of the above factors is relevant.<br>When DPIAs are carried out, controllers should document the purposes for processing and the security measures in place to protect data subjects. |

| Key issue | Changes introduced by GDPR |
|---|---|
| **In which circumstances are DPIAs not necessary?** | DPIAs may not be necessary when:<br>• it is considered that processing is not likely to result in a high risk to the rights and freedoms of data subjects<br>• a DPIA has already been carried out for a very similar processing operation (keeping in mind the nature, scope, context and purpose of the processing)<br>• when the processing operations have been checked by a supervisory authority before the coming into force of the GDPR and the circumstances have not changed<br>• where there is a legal basis for processing in EU or Member State law and a DPIA has already been carried out in order to establish this legal basis |
| **When should a DPIA be carried out?** | DPIAs should be carried out as soon as possible and before processing begins.<br>The DPIA may need to be reviewed once the process is finalised.<br>Controllers should continually monitor their processing activities to confirm the level of risk associated with this activity. |
| **What should a DPIA contain?** | As a minimum, a DPIA should contain:<br>• a description of the intended processing operation<br>• the purpose of the intended processing operation<br>• an assessment of the likely risks to the rights and freedoms of natural persons<br>• how the data controller will manage the risks<br>• how the data controller considers itself to be compliant with the GDPR |
| **Are data controllers required to publish their DPIA?** | This is not a requirement under the GDPR but the WP29 suggests that publishing the conclusion of a DPIA will help to demonstrate accountability and transparency. |
| **When should supervisory authorities be consulted?** | Supervisory authorities should be consulted when risks to data subjects are very high. For example, when processing health data on a large scale. |

In January 2017, the WP29 published a new set of priorities for providing GDPR guidance for 2017. The WP29 reiterated its commitment to finalise the guidelines started in 2016 and that were not adopted/finalised by the end of 2016, including:

- guidelines on the certification mechanism
- guidance on administrative fines
- setting up the EDPB structure in terms of administration (e.g. IT, human resources, service level agreements and
- budget); and
- preparing the one-stop-shop and the EDPB consistency mechanism

Additionally, the WP29 also committed to start assessments and provide guidance for:

- consent
- transparency

Furthermore, due to the changes introduced by the GDPR, WP29 plans to also update existing guidance published on international data transfers.

The Article 29 Working Party (WP29) has also published draft guidance which are open for consultation until 28 November 2017, on the following:

- personal data breach notification
  http://ec.europa.eu/newsroom/document.cfm?doc_id=47741
- automated individual decision-making and profiling
  http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963
- application and setting of administrative fines (for regulators)
  http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

While organisations can only welcome long-awaited and needed guidance on all the new concepts and practical changes brought by the GDPR, the allocation of responsibilities for the production and publication of the various GDPR guidelines between the WP29 and the national DPAs appears rather confusing in the eyes of EU businesses expected to rely on them to achieve compliance with the GDPR.

However, a couple of DPAs including the ICO in the UK and the CNIL in France have initiated consultations with a view to publish guidelines on consent this year (in May for the ICO) whereas the WP29 has also announced the publication of guidelines on consent in 2017. It is worth noting that the scope and questions submitted by the national DPAs as part of these public consultations are somewhat different, although it is understood that the outcome of these national consultations and/or guidelines will be taken into consideration for the issuance of the European guidelines on consent by the WP29.

Moreover, there has been and there may be further consultations/guidelines issued by the national DPAs on other topics. For instance, the Irish Data Protection Commissioner published its own first set of GDPR guidelines in 2016; the CNIL in France has launched a consultation due to close by end of March 2017, covering not only consent but also data breach notification and profiling. The Belgian Privacy Commission has launched a public consultation on its draft data protection impact assessment guidance which closed at the end of February 2017. On 26 January 2017, the Spanish data protection authority (AEPD) issued three guides for small and medium-sized companies on complying with the GDPR: a guide for data controllers, contracts between data controllers and processors, and the information obligations for controllers.

Clearly, all these DPAs' consultations and guidelines are running in parallel to the harmonisation work undertaken by the WP29 and raises concern as to the logic of such lack of coordination between the DPAs and the WP29.

One may question the reasons why the national DPAs' consultations and issuance of guidelines on the GDPR seem to take place ahead of the publication of the GDPR guidelines announced by the WP29 and why there has not been a concerted effort to align the overall process, content and calendar of the publication of the various GDPR Guidelines between the

national DPAs and the WP29. It is not clear why a reverse order of precedence was not adopted whereby the WP29 would have issued first the various promised guidelines and the national DPAs would then have had the opportunity to use common framework guidance for each topic and proceed with adaptations to the national specific requirements where possible.

Undoubtedly, further clarification and harmonisation of the consultation process on GDPR guidance followed by the WP29 and the DPAs is required sooner than later.

## For further information, contact:

Dr. Nathalie Moreno
Partner

+44 (0) 20 7074 8461
nathalie.moreno@lewissilkin.com