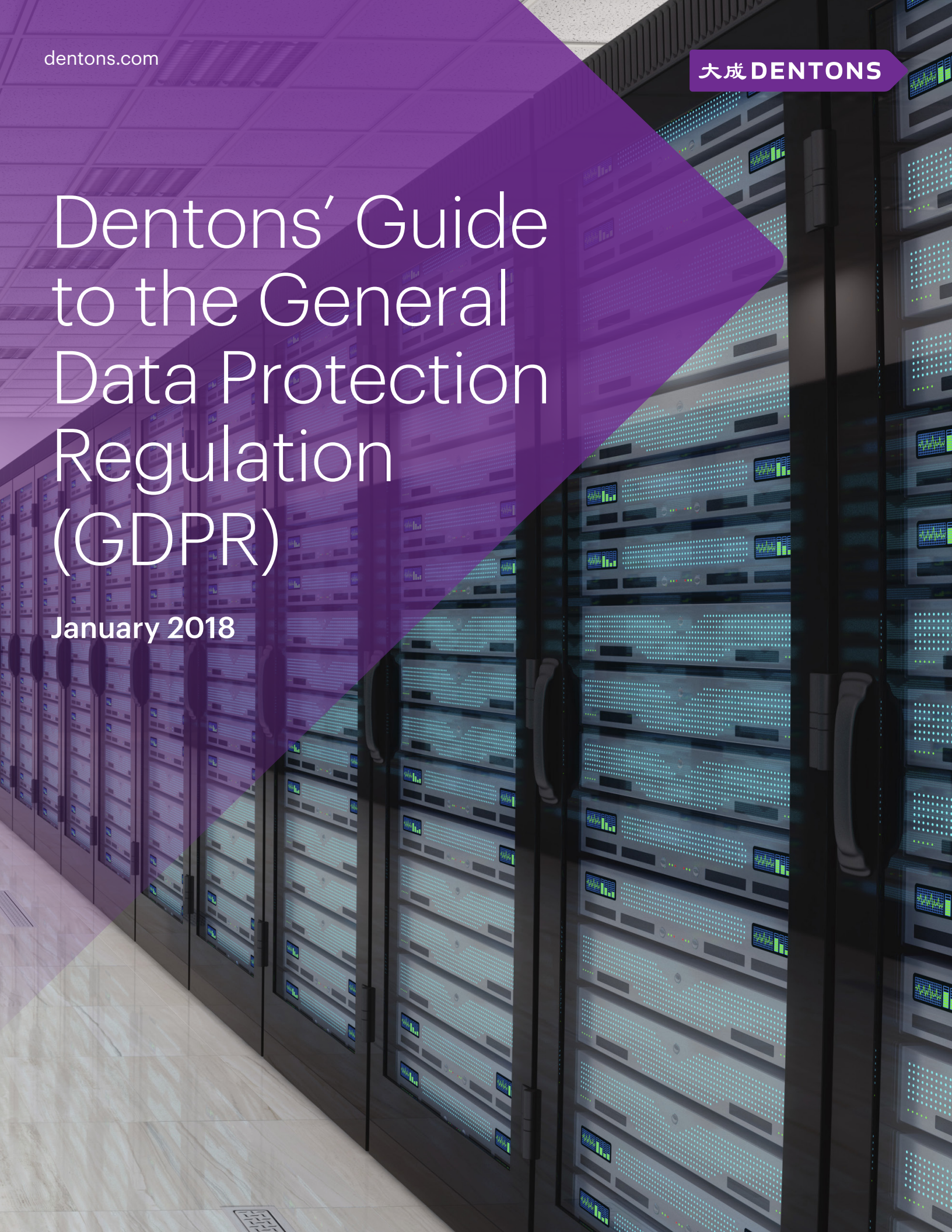
dentons.com

大成 DENTONS

Dentons' Guide to the General Data Protection Regulation (GDPR)

January 2018



Contents

Introduction

Current European data protection law is contained in the European Data Protection Directive (95/46/EC) (Directive). Each EU member state has implemented it in local law. The General Data Protection Regulation, coming into force on May 25, 2018, will replace the Directive and European local privacy laws, introducing an unprecedented level of data protection obligations for business worldwide having commercial activities in Europe.

The General Data Protection Regulation (GDPR) will repeal and replace current law. As the GDPR is a regulation, it will be directly applicable to European member states.

The GDPR will come into effect on **May 25, 2018.** There is no grace period and organizations will need to comply with the new rules from this date. Some member states have already adopted some GDPR requirements in local law.

The GDPR is a major overhaul of current law. One of the key changes is that Supervisory Authorities (the new name for Data Protection Authorities) can impose fines of up to **4 percent of global revenue or €20 million (approx. CA$30.7 million),** whichever is higher, for breaches of the GDPR. Specifically, the GDPR focuses on organizations having appropriate data protection governance in place with a real emphasis on accountability.

Purpose of this Guide

The purpose of this Guide is to highlight the main principles and changes under the GDPR. It is intended to be used by businesses as an aid to a GDPR fact find/audit, and to help anticipate likely practical steps required. Each section of this Guide describes a different principle and/or change under the GDPR. We have also set out suggested "Actions" to consider under each section. These "Actions" will help identify any gaps in compliance.

Please note that this Guide is not a comprehensive statement of the GDPR. We expect further guidance to be issued on the GDPR. This Guide doesn't cover Article 29 Working Party Guidance recently issued. Further laws may also be implemented (e.g., local laws), which need to be taken into account when assessing compliance.

Territorial scope

What is the territorial scope of the GDPR?

Similar to the current law under the Directive, the GDPR will apply to any organization that is "established" in Europe and which is processing personal data in the context of that establishment. According to the Recitals of the GDPR, "establishment" implies the effective and real exercise of activity through stable arrangements. For example, having a local representative or agent may be sufficient to trigger an "establishment".

Another major change introduced by the GDPR is that it has **extra-territorial effect.** The GDPR will also apply to an organization which is **not established** in Europe, but carries out the following processing activities:

- Offering goods or services (even if no payment is required) to individuals in Europe; or
- Monitoring the behaviour of individuals in Europe.

Offering goods or services to individuals in Europe

The mere accessibility of a website from Europe or the use of a language generally used in the country where the organization is located **does not** trigger the extra-territorial effect of the GDPR.

Factors, such as the use of a language or currency generally used in one or more EU member states, with the possibility of ordering goods or services in that other language, or the mentioning of customers or users who are in Europe, could trigger the extra-territorial effect of the GDPR. So if, for example, a website is "directed at" particular EU member states, the GDPR will apply.

Monitoring the behaviour of individuals in Europe

This includes the tracking of individuals for profiling purposes, particularly in order to take decisions concerning the individual, or for analyzing or predicting their personal preferences, behaviours and attitudes. This could apply in the context of online behavioural advertising.

Actions:

- Consider whether your organization is "established" in Europe and, therefore, triggering the GDPR. Which affiliates are caught by this test?
- Consider whether non-European entities (e.g., your US offices) are conducting activities (e.g., offering goods/services or monitoring behaviour), which could trigger the application of the GDPR.
- Specifically consider the content of your company's websites and whether this could trigger the application of the GDPR. Consider ring-fencing certain websites so their content is not "directed at" EU residents and they, therefore, remain off-risk.
- Create a process by which future processing activities and mergers/acquisitions are assessed to determine whether it may trigger the application of the GDPR.
- Consider segmenting your data to distinguish data sourced from the EU and data sourced outside the EU – so we can apply GDPR only as far as required.
- Where the GDPR applies to your organization (or part thereof), comply with the obligations as set out in this Guide.

Definitions

Key definitions: What's changed?

The GDPR has updated key definitions from the Directive, for example:

- "Personal data" has been expanded to explicitly call out "identifiers", such as device IDs, IP addresses, cookies, RFID tags, location data and genetic data;
- "Sensitive personal data" has also been widened to include genetic data or biometric data.
- Significantly, the GDPR has also defined "personal data breach" for the first time. Techniques commonly used as part of data collection and processing such as "profiling" and "pseudonymization" have also now been defined.

Summarized key definitions from the GDPR are set out below.

Key definition	Meaning
Personal data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This is a very broad definition and includes names and addresses, contact details, HR records and other identifiers, such as device IDs, IP addresses, cookies, RFID tags and location data.
Controller/Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the processes and means of the processing of personal data. This means the data owner, employer, operating company as applicable.
Processor/Data processor	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This means your vendors or service providers (whether external or affiliates).
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. This catches any internal or external breach of security as it relates to personal data.

Key definition	Meaning
Processing	Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Effectively, this means "doing anything with data".
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. This includes any form of profiling: cookie profiles, OBA, e-recruitment, psychometric testing and assessments used as gateway for onboarding customers or staff.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately, and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. This means a process of de-identifying data, hashing or applying dummy IDs to minimize it, and removing identifiers.
Special categories of personal data/sensitive data	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. This is higher risk data and requires additional protection (explicit consent usually and best practice security).

Actions:

- Generally, be aware of these expanded or new definitions and assess whether they will have any impact on your collection and use of data.
- Identify whether you hold any genetic or biometric data, as this is now explicitly considered "sensitive" and merits greater protection.
- Check if you undertake any "profiling" (as defined) and whether it constitutes automated decision-making, as individuals have rights not to be subject to automated decision-making in certain circumstances.
- If you carry out any pseudonymization of data, ensure that it meets the criteria set out in the GDPR definition.

Data Protection (DP) Principles

What are the DP Principles?

The DP Principles set out the main responsibilities for organizations and are contained in Article 5 of the GDPR. The first six are similar to those in the *Data Protection Act* but article 5(2) also adds a new "accountability" requirement. Each of the principles are stipulated below, with a summary of the key actions to help comply with each one also highlighted:

5(1): Personal data should be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

Actions:

- **Lawfulness:** At least one of the **conditions in Article 6** needs to be complied with – these include, the data subject giving consent, the processing being necessary to comply with a legal obligation or for the performance of a task carried out in the public interest.
- **Note:** For special categories of data, **additional conditions in Article 9** need to be complied with.
- **Transparency: Tell individuals** how their data is being processed, in a way that is **concise,** easily **accessible,** easy to **understand,** and in **clear and plain language.** Consider icons and "just in time" notices. Identify all current notices and refresh them.

(b) Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;

Actions:

- **Purpose limitation:** Determine the purpose at the time of collection.
- **Further purpose:** When processing is not based on consent, take the following into account to assess whether the further purpose is compatible: **link** between purposes, **context** of data collection, **nature** of personal data, **consequences** of further processing, and **appropriate safeguards.**

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Actions:

- **Data minimization:** Ensure you collect and retain the minimum data required. Consider pseudonymization.

(d) Accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

Actions:

- **Data accuracy:** Ensure all data is **accurate** and kept **up-to-date**. Clean databases.

(e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Actions:

- **Storage limitation:** Data controllers are encouraged to **set time limits.**
- **Public interest:** For data that is kept longer due to public interest, **Article 89(1)** needs to be complied with.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Actions:

- **Security:** Ensure appropriate **security measures** are put in place.

5(2) – The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Actions:

- **Accountability:** This is a new principle (compared to current data protection law).
- **Recommended measures:** To comply, data controllers should implement appropriate **technical and organizational** measures to ensure and be able to demonstrate compliance, including policies, procedures, training and awareness, appoint **a data protection officer** (where appropriate), and implement measures that meet the principles of data protection by design and data protection by default (which include **data minimization and pseudonymization).**

Transparency

What is "transparency"?

Organizations will need to provide detailed information to individuals about the processing of their personal data, specifying what data is processed (i.e., categories/types), why it is processed (i.e., purposes), how it is processed (i.e., what is done to the data), and where it is processed or sent to (including whether it is shared with other organizations).

What are the new transparency requirements?

The information to be provided is more extensive. New items include:

- Contact details of Data Protection Officer (DPO), if any;
- Legal basis for processing (e.g., "legitimate interests");
- Details on data transfers;
- Rights of erasure, restriction, portability and to object to processing;
- If processing is based on consent, right to withdraw consent;
- Right to lodge a complaint with a Supervisory Authority (SA);
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data; and
- Information about profiling based on automated decision-making (logic and consequences).

There are also additional requirements depending on whether personal data is obtained directly from the individual or not.

Information may be provided in combination with "standardized icons" that are to be published by the Commission.

Also, the timeframe within which the information must be provided to individuals is specified and varies depending on whether personal data is obtained directly from the individual or not.

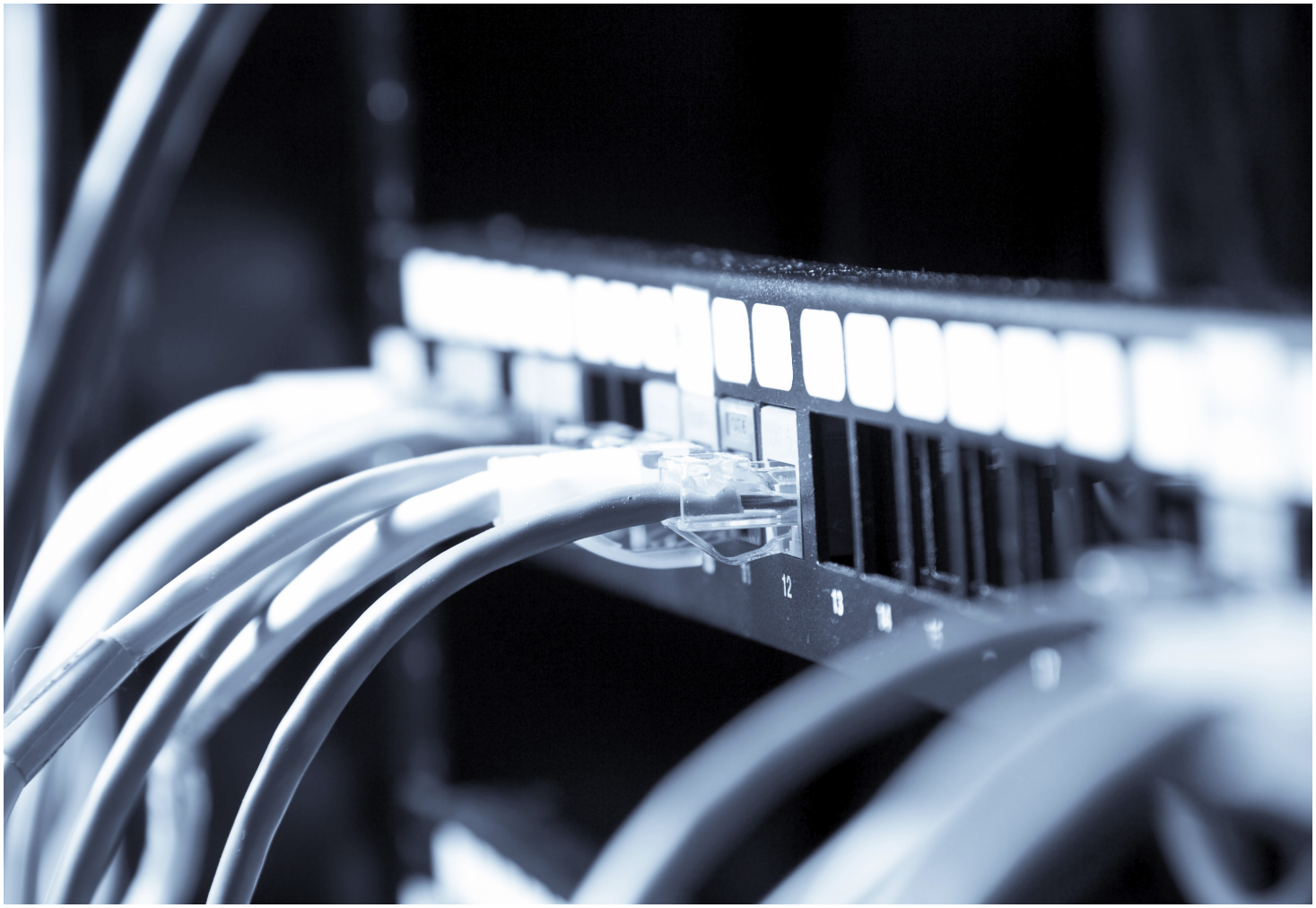
How will these changes affect us?

- Single, EU notice should be sufficient!
  - Makes drafting easier, as no member state variations.
  - Translations into local languages (still) required.
- BUT, much greater detail is required...
  - Although most of the additional information should not be too tricky to supply.
  - No guidance published yet on retention periods and legitimate interests disclosures.
  - There is a challenge for organizations that share data intra-group without any clear restrictions on use by other group entities. This may be difficult to describe in a notice.
  - Greater compliance risk will apply to organizations relying on third-party marketing lists – higher standard of due diligence required.

Actions:

- Review and update existing notices (employee and outward facing).
- Agree on a template notice and bespoke it for each channel: e.g., "in app"/website privacy policies, on-device notices, hard copy disclosures, call script, other.
- Prioritize version control / audit trail of the notices, and ensure consistency of content across the group.
- Work with group companies to assign responsibility for notice review, update and approval.
- Where relying on data collected indirectly, check that notice is given at the appropriate time.

Don't forget that failure to provide an adequate notice carries risk of a fine up to 4 percent of global annual revenue, or €20 million (approx. CA$30.7 million) (whichever is higher)!



Processing conditions

What are the processing conditions?

A key GDPR principle is to process information "lawfully". To achieve this, companies are required to satisfy a processing condition. There are processing conditions that apply to the processing of all or any personal data, and an additional set of conditions that apply to processing of special categories of data.

The most commonly-used condition is to collect consent from the individual. In cases of special categories of data, this must be explicit consent. The requirements for collecting valid consent are covered separately in this paper. We have set out the main processing conditions below.

Conditions: All personal data

We have set out a non-exhaustive list of conditions that companies can rely on to legitimize the processing of personal data (see Article 6, GDPR). Many of these already apply under the current law, but we have expanded on when these conditions may be used in practice. The conditions apply where **the data subject has given consent** or where the processing is necessary (and this means "essential"):

- For the **performance of a contract** with the individual or to take steps to enter a contract;
- For compliance with a **legal obligation:**
  - This must be an obligation applicable to the controller under EU / member state law. So, disclosure requests from US regulators are not necessarily covered;
  - The obligation also needs to be "clear and precise". This means companies cannot rely on blanket/informal obligations;
- To protect **vital interests:**
  - This should be used restrictively (e.g., "life or death" scenarios), and only where another suitable processing condition cannot be relied on;
- For the performance of a task carried out in the **public interest;**
  - The scope of this condition is unclear. The Recitals to the GDPR refer to where the task is carried out, or the authority of the controller is laid down under, EU or member state law;
- For the purposes of **legitimate interests** pursued by the controller, except where these interests are overridden by those of the data subject:
  - Companies are required to document the balancing exercise required to justify relying on this condition (e.g., is it within the reasonable expectation of the individual?);
  - The GDPR removes the possibility for public authorities to rely on this condition;
  - Relying on this condition to process children's data requires specific consideration (i.e., an assessment of the risks should be well-documented);
  - Reliance on this condition now needs to be documented in privacy notices.

Conditions: Special categories of personal data?

Commonly, companies obtain explicit consent when processing this type of information. However, we have set out a non-exhaustive list of alternative conditions to legitimize the processing of special categories of personal data (see Article 9, GDPR). Note, these conditions are **additional** (not alternatives) to relying on a condition for processing personal data (as set out above).

Conditions include where the processing is necessary:

- To carry out obligations under **employment, social security and social protection law;**
- To protect **vital interests** where the individual is incapable of giving consent;
- For the establishment, exercise or defence of **legal claims;**
- For **substantial public interest,** which is proportionate to the aim pursued;
- For certain **medical purposes** (e.g., preventative or occupational medicine);

- For **archiving purposes** in the public interest, **scientific** or **historical research** purposes or **statistical** purposes.
- Other conditions include, where:
  - The individual has deliberately made the information **public;** or
  - Processing is carried out by a **not-for-profit organization** about members / former members.

Actions

- **Identify** what processing conditions are being relied on to process personal data and special categories of personal data.
- **Validate** that these processing conditions still apply under the GDPR.
- "Legitimate interests" can potentially cover processing to prevent fraud, to ensure security or for the purposes of direct marketing.
- Where relying on the "**legitimate interests**" condition:
  - Ensure the reasoning to rely on this is **documented;**
  - Ensure it is within the **reasonable expectations** of the individual;
  - **Update privacy notices** to include information on where the "legitimate interests" condition has been relied upon;
  - If you are a public authority, seek an alternative processing condition; and
  - When processing children's data, conduct a detailed risk assessment and document this.

Consent

What is "consent"?

- Consent means any freely-given, specific, informed and unambiguous indication of the data subject's wishes. In certain cases, **explicit** consent is required, which means consent that is very specific as to data collected, purposes and disclosures. Under the GDPR, it will be more difficult to obtain or rely on consent.

When is consent likely to be relevant?

Consent is required in order to:

- Process personal data (unless you rely on another legal basis, such as "necessary for legitimate interests");
- Process special categories of data (e.g., racial or ethnic origin, political opinions, genetic or biometric data). This consent must be "explicit";
- Compile profiles about individuals on an automated basis where this produces legal effects. This consent must be explicit;
- Process children's personal data where parental/guardian consent may be required (online services and children under 16);
- Conduct direct marketing; and
- Collect cookie or device data.

Consent may also be required for data sharing (including intra-group), usage outside reasonable user expectations or other non-obvious purposes.

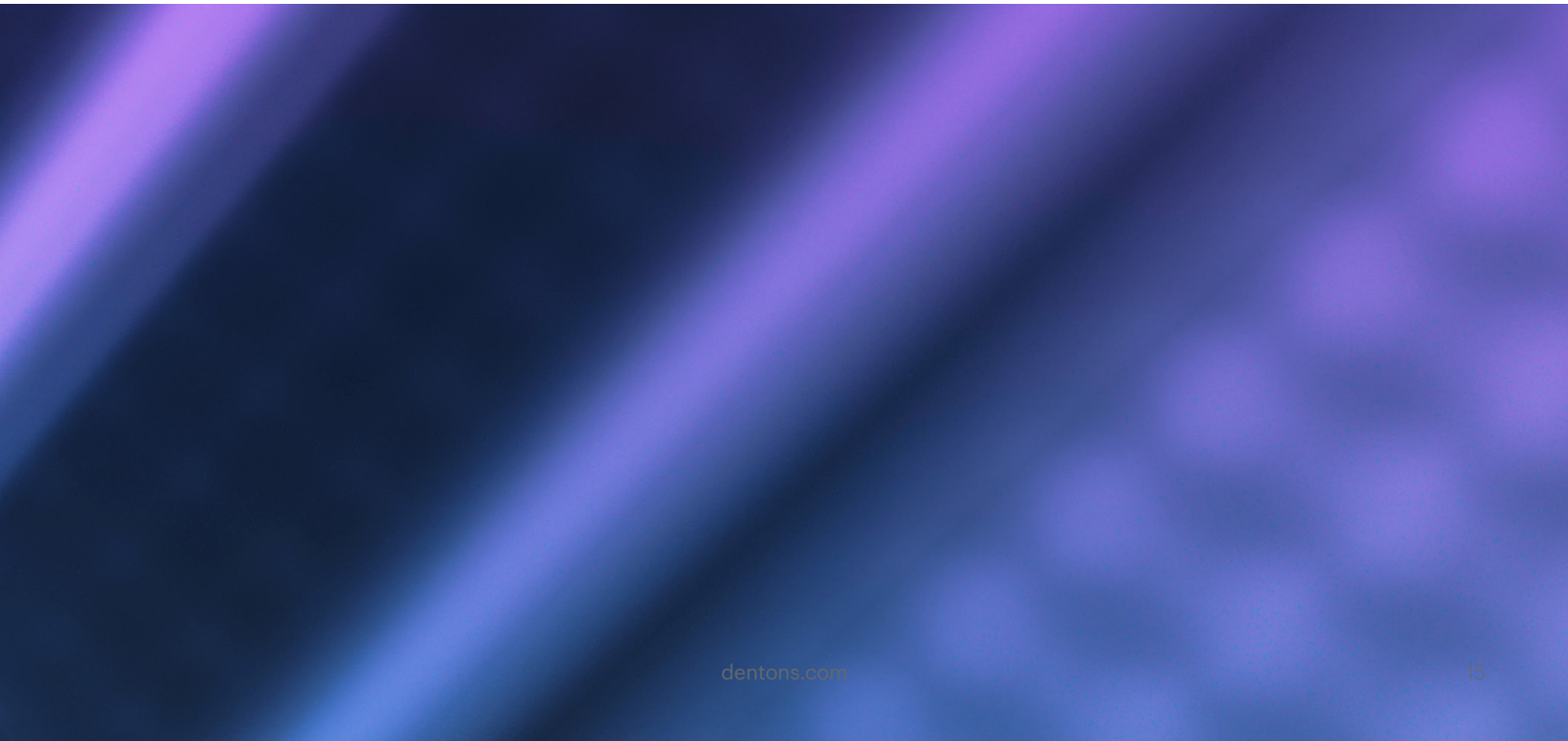
What are the new consent requirements?

In order to be valid, consent must:

- Be freely given – there must be a genuine choice for the individual. Consent should not be "bundled" or contingent on taking other goods or services;
- Be clear as to scope and extent;
- Include identity of the controller and the purposes (as a minimum);
- Include a clear affirmative action or statement by the user (this makes implied consent difficult);
- Be recorded in an audit trail;
- Be subject to a right to withdraw at any time;
- Not involve a clear imbalance between the controller and the individual (employer/employee).; and
- Be intelligible, easily accessible and in clear and plain language.

Actions:

- Identify all legacy consents currently in place and purposes for which consent is relied on.
- For each form of legacy consent, identify consent wording, scope and mechanics (i.e., what actions the user takes to evidence consent).
- Identify any required consents for future business changes or new products.
- Agree on consent strategy and template wordings.
- Avoid pre-ticked boxes or assumption that "silence is consent".
- Assume that user will need to check a box, sign a document or confirm consent orally.
- Agree on strategy on legacy consents (whether to refresh or not).



General rights

General

- Data subjects' existing rights are substantially strengthened under the GDPR.

Subject access rights

- Categories of information which must be provided in response to a data subject access request are more extensive.
- Beyond receiving confirmation that their data is being processed and access to such data, a data subject has the right to obtain other information, such as recipients in third countries, information on the right to complain to a supervisory authority and safeguards used for overseas transfers.
- Controllers must respond without undue delay and within one month at the latest. This is shorter than the current 40-day deadline applicable in the UK. Controllers must usually provide the information free of charge.
- If the request is made electronically, the personal data must be provided in a commonly-used electronic form.
- The exemptions from the duty to comply no longer provide for a "disproportionate effort" exception to providing hard copy information.

Right to rectification

- Data controllers must rectify inaccurate data and provide a supplementary statement if data is incomplete.
- This must be done free of charge and, generally, without undue delay and, at the latest, within one month. Data controllers must give reasons if they refuse the request.

Right to object

The right to object has been strengthened, but is still not a general right.

- Data subjects can object to processing based on legitimate interests or on the performance of a task in the public interest/ exercise of official authority (including profiling), direct marketing (including profiling) and processing for scientific/ historical research or statistics.
- The right to object to direct marketing is the only absolute right to object. For example, if a data subject objects to processing, which is based on legitimate interests, a controller does not need to comply with the request if they have compelling legitimate grounds for the processing. But this is a high bar and puts the burden of proof on the controller.

Right to restrict processing

- When processing is restricted, a controller is permitted to store the personal data, but not to further process it. The controller can retain enough information about the data subject to ensure that the restriction is respected in future.
- A data subject can "restrict" processing of personal data relating to them in circumstances where they have requested restriction for unlawful processing, contested the accuracy of the data, objected to the processing (and the controller is determining whether they have "compelling legitimate grounds" to keep processing) or if they require the data to establish, exercise or defend a legal claim (but it is no longer needed by the controller).
- If a controller has disclosed the personal data to third parties, it must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Actions:

- Assess whether there are adequate request mechanisms in place for the various data subject rights and if any mechanisms need to be updated (e.g., triggers for responding to subject access requests within the new time frame of one month).
- Implement IT upgrades, where required, for responding to individual rights.
- Be prepared for individuals to more vigorously exercise their rights under the GDPR. Produce new template response letters for enhanced rights (e.g., rectification), and consider whether existing letters for responding to data subject right requests need updating.
- Consider whether additional tools/resources (e.g., to respond to an access request in electronic form or to contact third party data recipients in respect of rectification of data) are necessary.
- Consider training and workshops to "upskill" those responsible for dealing with or likely to receive data subject right requests. This could include HR and Customer Support teams.
- Data retention strategy is relevant here. A rigorous approach to deleting data once it is no longer needed could minimize the effect of these enhanced rights.

Right to be forgotten

What is the "right to erasure"?

Article 17 of the GDPR provides data subjects with a right to request the erasure/deletion of their personal data in certain circumstances.

The purpose of the right is to enable individuals to stop data about them being processed where it is no longer relevant or appropriate. The right is not an absolute right, as there are qualifying conditions which must apply, as well as exemptions.

The qualifying conditions

The right to erasure applies only where the:

- Personal data is no longer necessary for the purposes for which it was collected/processed;
- Data subject withdraws their consent (assuming this is the condition on which the processing is based), and there is no other legal ground for the processing;
- Data subject objects to the processing and there is no overriding legitimate grounds for the processing, or the data subject objects to their personal data being processed for direct marketing purposes;
- Personal data has been unlawfully processed (e.g., in breach of the GDPR);
- Personal data has to be erased for compliance with a legal obligation under European law to which the data controller is subject; or
- Personal data of children has been collected as part of online services.

Compliance conditions

- The data controller must respond without undue delay and in any event within one month of receipt of the request.
- Where the data controller has made the personal data public, and is obliged to erase the data, the data controller must take reasonable steps (including technical measures) to inform others processing the personal data, that the data subject has requested erasure of that data. This obligation strengthens an individual's right to be forgotten in the online environment.

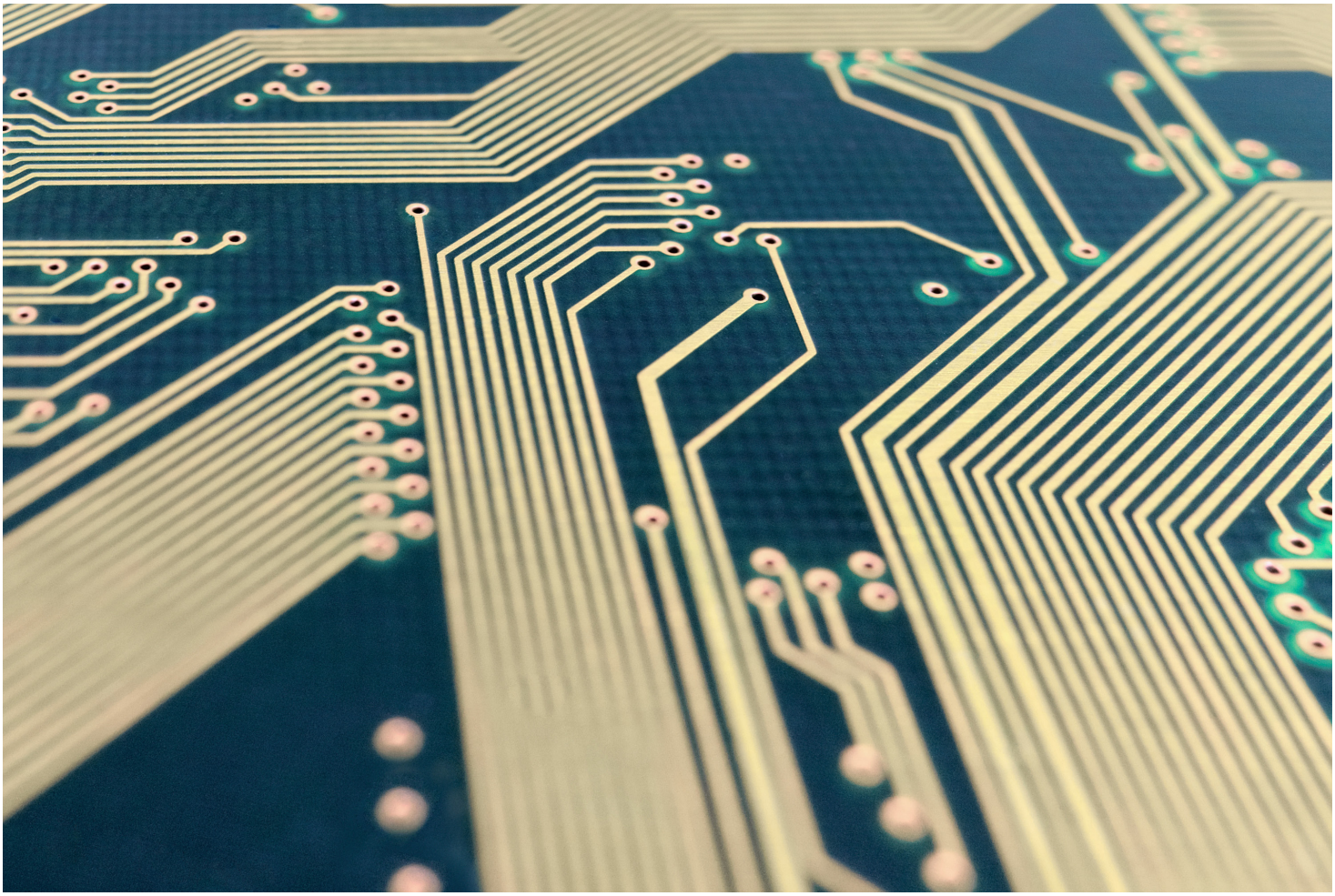
Exemptions

The right cannot be exercised where the processing is necessary for:

- Exercising the right of freedom of expression and information;
- Compliance with a European legal obligation that requires the processing;
- Performance of public interest or exercise of official authority;
- Public health reasons;
- Archiving, scientific or historical research purposes, or statistical purposes; or
- The establishment, exercise or defence of legal claims.

Actions:

- Train staff to recognize and act promptly upon receipt of a request for data erasure from a data subject so that the limited time for responding is not wasted.
- Review processes and procedures to establish whether they address issues relating to data erasure.
- Review how data will be searched and filtered in response to a request. Do we have technical limitations on functionality to erase data across systems including back-up? This may require a system upgrade to allow for quick deletion.
- Consider the effect on multiple copies of personal data in different parts of the system.
- Consider if, and how, it is possible to assess whether data relates to more than one individual. Consider mechanisms to deal with data that does relate to more than one individual (obtaining consent, isolating data, etc.)
- Develop mechanisms/policies dealing with notifying others where data has been made public or shared with other data controllers.
- Put in place a means to keep an audit trail of requests and steps taken to comply with a request.



Right to data portability

What is data portability?

- The new data portability right gives an individual the right to require that a data controller provides to that individual the information it holds concerning that individual in a "structured, commonly-used and machine-readable format" or to require the data controller to transmit that data to another data controller "without hindrance".

- The purpose of the right is to empower individuals by providing them with the ability to move, copy or transmit their data from one IT environment to another, giving them more control over their data. So a customer can "port" their data to another supplier or competitor easily.

The qualifying conditions

The right to data portability applies only:

- To personal data processed by automated means (it does not apply to paper records); and

- To personal data that the individuals themselves have provided. This likely includes data generated by the individual's activity but not inferred data derived by the data controller from subsequent analysis of the data provided by the individual; and

- Where the basis for processing was:

  - Consent / explicit consent; or

  - Where the data is being processed to perform a contract or in connection with steps preparatory to a contract.

The right does not apply if processing is based on one of the other grounds for lawful processing, such as compliance with a legal obligation or performance of a task carried out in the public interest.

Compliance conditions

- The data controller must inform the individual of the availability of the rights at the time data is collected from the individual.

- The data controller must respond to the data subject (or notify the individual that it is refusing to comply with the request) without undue delay and, in any event, within one month of receipt of the request. This period may be extended (by an additional two months), if justified by the complexity and number of requests. If the data controller intends to exercise its rights to extend the period, it must notify the individual within the initial month, and set out the reasons for the delay.

- Where a data subject makes a request by electronic means, the controller should respond by electronic means where possible.

- Compliance with the rights shall be free of charge unless the request is manifestly unfounded or excessive. The burden is on the data controller to demonstrate this. The overall cost of the processes required to answer data portability requests should neither be taken into account to determine the excessiveness of the request, nor be used to justify a refusal to answer portability requests.

- The rights are without prejudice to the rights of other data subjects (e.g., where providing data would adversely affect the rights of the other individuals).

The transfer of the data

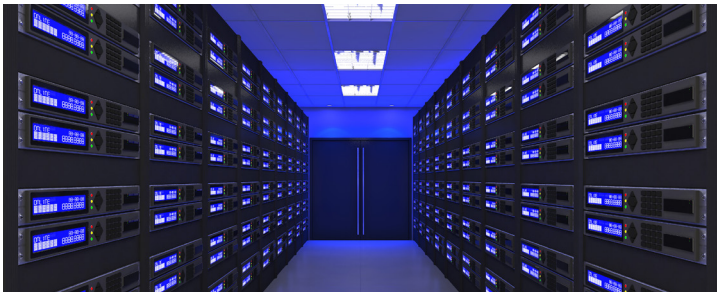
- The individual is entitled to continue to use that data controller's service after the supply of a copy of the data by the data controller in accordance with this right.

- The GDPR envisages that data controllers should be encouraged to develop interoperable formats to enable data portability, but it acknowledges that the right does not create an obligation for data controllers to adopt processing systems which are technically compatible. The minimum requirement that personal data must be provided in a "structured, commonly-used and machine-readable format" should facilitate the interoperability of the data format provided by the data controller. The aim is interoperability, not compatibility.

- The data controller receiving the data will be responsible for ensuring that the data received is relevant and not excessive with regard to that controller's proposed processing.

Actions:

- Train staff to recognize and act promptly upon receipt of a request for data portability from a data subject so that the limited time for responding is not wasted.
- Review processes and procedures to establish whether they address issues relating to data portability.
- Consider if, technically, data is held in a manner which can be exported in a structured, commonly-used, machine-readable format. How will we do this?
- Review how data will be searched and filtered in response to a request.
- Consider if, and how, it is possible to assess whether data relates to more than one individual. Consider mechanisms to deal with data that does relate to more than one individual (obtaining consent/isolating data etc.).
- Develop mechanisms/policies dealing with the acceptance of data from the data subject/third parties where the third party has exercised its portability rights and wishes to have that data transmitted to you.
- Put in place mechanisms to ensure that any data you deliver in accordance with this right is secure and delivered to the right person. This could include the use of encryption and additional authentication information.



“Dentons gives incredibly practical advice for businesses and is able to provide very up-to-date insights on recent regulatory developments in data protection.”

Band 1 - Data Protection *Chambers* 2017

Data Protection Officer

How does the GDPR address this issue?

The GDPR introduces a requirement for some organizations to appoint a Data Protection Officer (DPO) to oversee their organization's data protection activities, and compliance with the GDPR.

When is this likely to be relevant?

Compliance with the GDPR requires an organization to appoint a DPO where the controller is a public authority, or the controller's activities require **regular and systematic monitoring** of data subjects on a large scale, or its core activities consist of processing on a large scale **special categories of personal data** or data relating to criminal convictions and offences.

What are the new requirements?

The DPO must have sufficient expert knowledge of data protection law and practices. The necessary level of expert knowledge should be proportionate to the type of processing which the organization undertakes and the level of protection the personal data requires. Certifications or qualifications (e.g., CIPP/E) would be considered a way of evidencing sufficient knowledge.

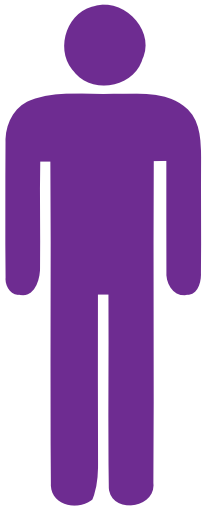
The DPO can be a staff member (including an existing staff member) or an externally appointed person, as long as there is no conflict of interest.

Organizations appointing a DPO must ensure:

- The DPO reports to the highest level of management (i.e., Board level);
- The DPO can operate independently, and is not dismissed or penalized for performing their duties;
- Adequate resources are provided to enable the DPO to fully perform the required duties.

The DPO must, at a minimum:

- Inform and advise the organization and its employees about their obligations to comply with the GDPR and other data protection laws;
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits; and
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).



Actions:

- Consider who would be an appropriate Data Protection Officer within your organization.
- Assign responsibility and budget for data protection compliance within your organization.
- Consider reporting lines and what training will be necessary.
- Implement the necessary support to allow the Data Protection Officer to perform the required duties as detailed above.

Privacy by design/default

The GDPR expressly legislates for what has been considered best practice in data governance. Among the new data governance obligations are the obligations of:

- **Privacy by design:** To take appropriate measures to integrate the GDPR's data protection principles into data processing operations – taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the severity and likelihood of the risks posed to privacy. This includes, for example, pseudonymization. This obligation applies to existing and new processing.
- **Privacy by default:** To take appropriate technical and organizational measures to minimize the use of data, with regard to each specific purpose of processing, as the default position. Minimization applies to the amount of data collected, extent of processing, storage period, and accessibility. In particular, personal data should not be made accessible, without the individual's intervention, to an indefinite number of other individuals. This also applies to existing and new processing.
- **Conducting Privacy Impact Assessments (PIAs):** To identify and minimize the risk of non-compliance. PIAs (also known as DPIAs) are required, in particular, where the processing involves:
  - The systematic and extensive evaluation of personal information based on automated processing (including profiling), and such evaluation significantly affects the person or has a legal effect;
  - Large-scale use of special categories of data or criminal conviction data;
  - Systematic monitoring of a publicly-accessible area on a large scale.
- This is most likely to impact on e-recruitment, credit assessment, large-scale processing of special categories of data or criminal convictions, large-scale CCTV or other monitoring of a public area. But this is not an exhaustive list.

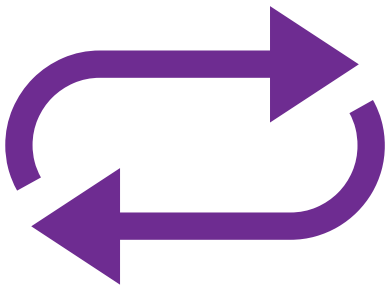
As a minimum, the PIA (or DPIA) must contain:

- A systematic description of the envisaged processing, its purpose and (if applicable) the legitimate interest justifying it;
- An assessment of the necessity and proportionality of the processing in relation to the purposes;
- An assessment of the risks of harm posed to individuals; and
- The measures envisaged to address those risks and demonstrate compliance with the GDPR.

The Data Protection Officer should advise on the assessment. Where appropriate, the data subjects or their representatives should be consulted. If the risk is high and unmitigated, the controller must also consult the Supervisory Authority. This applies to new processing, especially using new technologies. The assessment should be reviewed at least where the processing involves a change in risk.

The GDPR requires contracts between controllers and processors to oblige the processor to assist the controller in complying with these measures, taking into account the nature of the processing and the information available to the processor.

Approved Certification Marks may demonstrate compliance with the above obligations and adherence to an approved Code of Conduct may help demonstrate compliance with the obligation to conduct privacy impact assessments.



Actions:

- Review existing and new processing operations and data flows to ensure that privacy design is built in and data minimization is observed, listing the data protection principles.
- Keep a record of the analysis.
- Ensure that your compliance program requires, in relation to all new processing, a decision as to whether a privacy impact assessment is required, and guidance as to when it is required, how it is carried out, what the outcome should be, how the ultimate solution is chosen, and when the Supervisory Authority must be consulted. PIAs (DPIAs) should address business and compliance risks as well as privacy risks. This process should be built into the planning stage of all new operations.
- The program should schedule regular reviews to ensure the above obligations continue to be met.
- Identify stakeholders (e.g., project and senior management, designers, IT and procurement, suppliers, PR, HR, compliance, users, externals) in your organization who should contribute to and approve PIAs.
- Train relevant personnel in the minimization of data and design and use of processing systems.
- Impose on suppliers an obligation to assist you in taking the above measures where appropriate.
- Monitor available Certifications and Codes of Conduct for suitability for use.
- Monitor EU guidance (Article 29 Working Party / European Data Protection Board) and local regulators – guidance on high-risk processing is in the pipeline.

Records of processing

How does the GDPR address this issue?

As part of its focus on accountability and good data protection governance, the GDPR requires organizations to maintain internal records of their processing activities. These obligations are somewhat similar to the "registrable particulars" under the *Data Protection Act,* which must be provided to the ICO.

When is this likely to be relevant?

For data controllers and processors:

The new requirements vary depending on the size of the organization. If your organization has more than 250 employees, internal records must be kept of **all processing activities.**

If your organization has fewer than 250 employees, records are **only necessary for higher risk processing** (i.e., the processing it carries out is likely to result in a risk to the rights and freedoms of the data subjects; this may include processing medical data, or children's data, for example).

For data processors:

All data processors will be obliged to maintain data processing records, regardless of size.

What are the new requirements?

For data controllers:

The following must be included in any record of processing:

- Name and details of your organization (and, where applicable, of other controllers, your representative, and data protection officer);
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Retention schedules, and
- Description of technical and organizational security measures.

For data processors:

The following must be recorded:

- Name and contact details of the processor, and of each controller on whose behalf the processor acts. Where applicable the details of the controller's and processor's Data Protection Officer should be included:
  - Categories of processing carried out on behalf of each controller;
  - Details of any transfers to third countries, including documentation of the transfer mechanism safe-guards in place, and
  - Description of technical and organizational security measures.

Actions:

- Consider whether you are a data processor or a data controller, and which of the obligations apply to your organization.
- Prepare records of your organization's processing activities. This may entail a review of how data is handled within your organization.
- Implement measures to ensure records of processing are updated regularly in the event of a regulatory audit.

Children

Processing children's data

What is "children's data"?

The GDPR repeatedly underlines the importance of protecting children. New requirements are introduced to ensure children are subject to extra safeguards.

Although the legislation offers no overarching definition of what constitutes children's data, any data relating to a child below the age of 16 can be considered to be children's data, and should be treated as such.

When is children's data likely to be relevant?

If an organization offers an "information society service" (i.e., targets online services) directly at children, certain requirements apply.

What are the new requirements for processing children's data?

Children are considered to merit specific protection with regard to their personal data under the GDPR, since they may be less aware of the risks, consequences and safeguards associated with data processing. Such protections apply in particular to the use of personal data for marketing, or creating personality or user profiles.

Consent

When offering services directly to an individual below the age of 16 (individual member states will be able to lower this threshold to the age of 13 if they choose to), and using consent as the legal ground for processing, it will be necessary to collect consent from the child's parent or guardian.

The GDPR requires organizations to also make reasonable efforts to verify that consent has been given by the parent or guardian, in light of available technology.

Notice

Building upon the GDPR's requirements for increased transparency, the legislation provides that notice provided specifically to children should be written in clear, concise and transparent language that a child could understand. The term "child" is not defined in this instance, so organizations should therefore be prepared to address these requirements in any notice aimed at teenagers.

Actions:

- Consider whether the new requirements are likely to affect you. If so, consider whether children's data is processed for marketing purposes, or to build a user/personality profile.
- If your organization offers services directly to children, assess which rules apply and ensure that appropriate parental consent mechanisms are implemented, including a verification process.
- Remain aware of national legislation, and whether the country in which you operate elects to lower the threshold of parental consent. Member states can reduce the threshold from 16 to 13.
- Where services are offered directly to children, ensure notices are drafted clearly and are easily understandable.
- Where relying on "legitimate interests" to justify processing children's data, ensure this is supported by a documented assessment to evidence that the right balance has been struck between the child's interests and those of your organization.

Security

How does the GDPR address security issues?

The GDPR requires controllers and processors to adopt certain security measures to prevent against, and mitigate the consequences of, data breaches. Currently this only applies to controllers so this is an area where processors are assuming statutory risk for the first time.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

When is this likely to be relevant?

The GDPR's security requirements will be relevant to all organizations, but particularly those for whom a security breach would likely result in a high risk to the "rights and freedoms" of individuals. The GDPR also introduces new requirements for data processors, who were not previously subject to the *Data Protection Act*.

What are the new security requirements?

The GDPR requires all data controllers and processors to implement, according to the level of risk associated with their processing activities, all appropriate technical and organizational measures to ensure data is protected. These can include pseudonymization, encryption, back-up data sets, etc. The GDPR requires controllers / processors to regularly test and assess the efficacy of these measures, and you can demonstrate compliance via codes of conduct and policies.

The GDPR also requires all controllers to maintain a register of all data breaches, comprising the details of the breach, its effects, and any action taken. This will demonstrate compliance in the event of an audit.

What does the GDPR require of organizations?

The GDPR introduces a duty on all organizations to report data breaches to the relevant supervisory authority and, in certain cases, to the individuals affected.

When reporting a data breach, the organization must outline the following:

- Nature of the breach, including (where possible) the categories and number of individuals affected, as well as the categories and number of personal data records concerned;
- Name and contact details of the organization's Data Protection Officer (or other contact) where more information may be obtained;
- Likely consequences of the breach; and
- Measures taken (or proposed to be taken) to address the issue, and any measures taken to mitigate adverse effects.

In case of a data breach:

- Data processors must notify the data controller without undue delay in the event of any data breach, as soon as they become aware of it.
- **Data controllers** must notify:
  - **The relevant supervisory authority** without undue delay (and no later than 72 hours) after becoming aware of a data breach. The data controller is exempt from this requirement if the breach is unlikely to result in a risk to the rights and freedoms of individuals. Most data breaches will need to be notified!
  - **Data subjects** without undue delay after becoming aware of the breach. The data controller is exempt from this requirement if any of the following conditions apply:
    - The controller has implemented security measures to ensure the data is unintelligible to anyone not authorized to access it (e.g., the data is encrypted);
    - The controller has taken measures to ensure the high risk to individuals is no longer likely to materialize, and
    - Notifying the individuals concerned would involve disproportionate effort. In this instance a public communication, or similar, would suffice, provided the individuals concerned are informed in an equally-effective manner.

Actions:

- Consider whether your organization is a data controller or a data processor.
- Consider the level of risk associated with a data breach within your organization, and your organization's exposure to a "high-risk" data breach (i.e., whether you process sensitive personal data, medical data, children's data, etc, and in what volume).
- Review the technical and organizational measures currently in place to ensure the protection of personal data, and assess whether these are adequate.
- Review the procedures for testing and assessment of security, and assess whether these are adequate.
- Ensure protocols are in place to ensure staff are trained to recognize and act upon any data breaches.
- Develop and implement a Data Breach log if you have not already done so.
- (If a data controller) review any third party agreements with data processors to ensure any data breaches are agreed to be reported to you without undue delay.

Processors

What / who are "processors"?

Processors are the entities processing personal data on behalf of controllers. Processors can be natural or legal persons, public authorities, agencies or other bodies. Essentially, any person or organization processing personal data on behalf of a controller will be considered a processor.

Examples of processers include IT service providers (such as providers of CRM solutions, cloud storage and DR / back-up services), and HR outsourcing organizations (such as providers of payroll, benefits and pensions services). Affiliates can also act as processors.

Under current law (i.e., not GDPR) processors are "off-risk". Processors do not currently owe any statutory duty to the individuals whose personal data they process. This position changes significantly under GDPR.

Requirements prior to engaging processors

GDPR requires controllers to take great care when selecting and engaging processors. Controllers must only select processors which:

- Provide sufficient guarantees for implementing technical and organizational measures to ensure processing meets the requirements of GDPR and protects individual rights;
- Only engage sub-processors pre-approved by the controller; and
- Enter into a contract with the controller which satisfies the requirements of GDPR and which sets out the:
  - Subject matter and duration of the processing;
  - Nature and purpose of the processing;
  - Types of personal data and categories of data subjects; and
  - Obligations and rights of the controller.

Processor contracts

GDPR contains prescriptive requirements regarding the detail of what must be covered in a contract with a processor. The key requirements include the following (this is not an exhaustive list):

- The processor may only process data on documented instructions;
- Persons authorized to process the personal data must be subject to obligations of confidentiality;
- The processor must implement measures to ensure a level of security appropriate to the risk (e.g., including encryption and pseudonymization of data) and assist the controller in meeting its security obligations;
- The processor must provide information and contribute to audits to demonstrate compliance ;
- The processor must assist the controller, should the controller require approval from a regulator regarding its processing activities; and
- The processor must implement measures to assist the controller in complying with the rights of data subjects.

Processor obligations

For the first time under data protection law, processors will have their own statutory obligations. The key obligations of processors under GDPR include the following (this is not an exhaustive list):

- Maintain records of processing activities which include:
  - Details of the categories of processing being carried out;
  - Details of any international transfers of personal data, including details of the relevant safeguards in place; and
  - A general description of the security measures in place to protect personal data;
- Cooperate with requests from regulators when requested;
- Notify controllers of data breaches without delay; and
- Appoint a Data Protection Officer if the processor meets the relevant criteria.

Processor liability

Beyond the contractual liability to controllers to which processors are exposed, current data protection law does not impose any liability on processors. Under GDPR, processors will have direct liability to data subjects.

If a processor's processing activities have caused harm to an individual and it can be shown that the processor has: (i) not complied with its processor obligations under GDPR; or (ii) acted outside the instructions of the controller, the processor will be liable to that individual for the damage caused.

It should be noted that controllers and processors may also be held jointly and severally liable to data subjects for the entire damage where they are involved in the same processing causing harm. Harm includes non-pecuniary loss, such as distress. Controllers or processors (as relevant) can claim back the amount paid to data subjects which corresponds to the harm caused by the other party.

Actions:

- For controllers:
  - Conduct data protection due diligence on data processors prior to engagement.
  - Identify key contracts with key third party processors and assess for compliance with GDPR requirements / data transfer solutions, like Privacy Shield.
  - Prepare template GDPR-compliant clauses to insert within agreements with processors.
  - Monitor security measures of data processors to assess for continued compliance with GDPR requirements.
  - Monitor appointment of sub-processors by the processor to assess for possible non-compliance risks.
  - Agree on liability position with the processor in the processing agreement to avoid the need for court action to settle disputes relating to joint and several liability claims.
  - Require processors to adhere / engage with your breach response policy and procedures.
- For processors:
  - Prepare template GDPR-compliant sub-processor agreements.
  - Maintain records of processing activities in line with GDPR requirements.
  - Periodically review and assess security measures for compliance with GDPR requirements.
  - Ensure international transfers of personal data are executed in line with an approved transfer mechanism (e.g., model clauses, Privacy Shield, BCRs, etc.).
  - Assess whether it is necessary to appoint a DPO.

Data transfers

Transfer restrictions

There is a general restriction on transferring personal data outside the European Economic Area (EEA). The GDPR confirms this rule but removes certain administrative requirements.

The most significant change is that the GDPR abolishes the requirement for the Standard Contractual Clauses (Model Clauses) to be notified or authorized by Supervisory Authorities. The GDPR also, for the first time, provides a statutory footing for Binding Corporate Rules.

Adequate countries

The European Commission has the power to determine that "third country" provides adequate protection for personal data. Where data is transferred to such a country, no further measures need to be put in place.

Canada (and 10 other countries, but not the US) is recognized to provide an adequate level of protection for personal data. This list will remain in force once the GDPR is effective. However, Canada's status will come under review within four years of the entry into force of GDPR. Until then, Canadian companies will continue to enjoy the competitive advantage of being able to receive personal data from the EEA without specific authorization.

Data transfer solutions

Should it be necessary for transfer to a third state, there are certain measures which can be put in place in order to transfer personal data without prior approval from a supervisory authority. This is where the transfer is based on:

- A legally-binding and enforceable instrument between public authorities or bodies;
- Standard data protection clauses adopted by the European Commission or adopted by a Supervisory Authority (and approved by the European Commission);
- Binding corporate rules (suitable for intra-group data transfers only). This still requires approval from supervisory authorities; however, this has to be determined by a consistency mechanism;
- An approved code of conduct which is binding on the parties;
- An approved certification mechanism, which is binding on the parties; and
- The EU/US Privacy Shield (only applicable for transfers to the US). This is the replacement solution for the Safe Harbor regime, which was invalidated in October 2015. The Privacy Shield is not expressly referenced in the GDPR, but it is recognized by the European Commission as providing adequate protection.

Existing data transfer solutions

Existing data transfers based on the Standard Contractual Clauses approved by a data protection authority and other "adequacy" decisions by a data protection authority will continue to be valid until amended, replaced or repealed by the Supervisory Authority.

Derogations

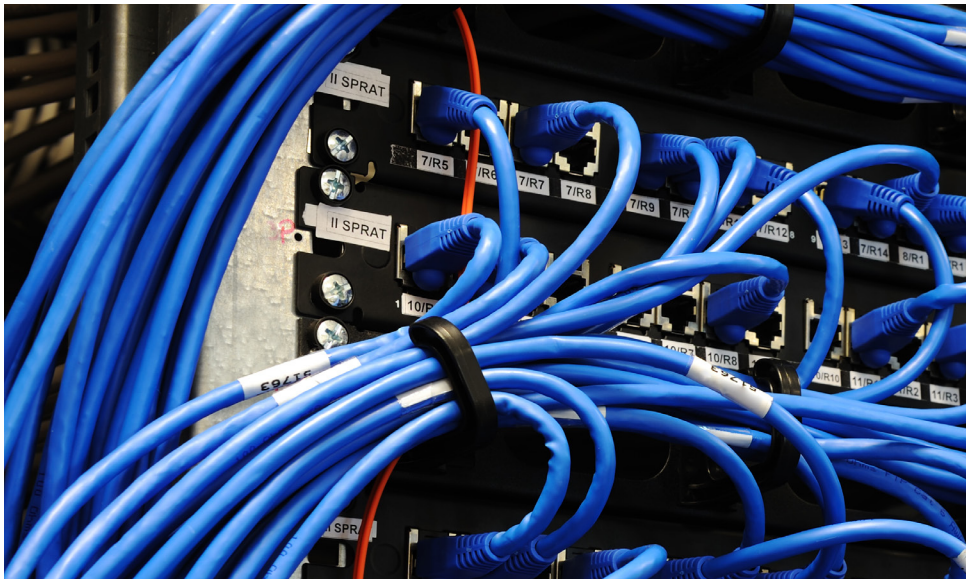
There are a number of derogations which allow the transfer of personal data outside the EEA in limited circumstances. Some examples of these derogations are:

- Where the explicit and fully-informed consent of the individual is obtained;
- The transfer is necessary for the performance of a contract between the data subject and the data controller;
- The transfer is necessary for public interest reasons; and
- The transfer is necessary for the establishment, exercise or defence of legal claims.

Where the transfer of personal data cannot be based on: (i) an adequacy finding; (ii) a data transfer solution; or (iii) a derogation, then, in limited circumstances, a transfer can be made on the basis of "compelling legitimate interests" pursued by the data controller. This only applies where the transfer is not repetitive and concerns only a limited number of data subjects. The data controller must also assess all the circumstances surrounding the data transfer to ensure that suitable safeguards are in place. The data controller must also inform the supervisory authority and the data subjects of the transfer.

There are also rules under Article 48 to prohibit the transfer of personal data outside Europe, pursuant to non-EU legal requirements or Court Order, except under an MLAT or equivalent international agreement. MLATs are a

very slow way to legitimize the transfer of data! This creates a practical difficulty where you are required to comply with a US Court Order but compliance with it may breach Article 48 of the GDPR. The UK plans to derogate from this (so it should not be an issue in the UK) but it will be an issue elsewhere in the EU.



Actions:

- Audit data flows and produce data flow map.
- Determine which data transfer solution(s) is/are being relied on for transfers outside the EEA.
- Conduct audit of vendors to establish where personal data is being processed.
- Upgrade any data transfer solutions relying on Safe Harbor.
- Ensure that processes are set up so that new data flows and vendors processing data on your behalf are assessed on an on-going basis.

Contacts

Canada

Chantal Bernier
Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

China

Ken Dai
Partner, Shanghai
D +86 21 5878 5888
jianmin.dai@dentons.cn

Jet Deng
Senior Partner, Beijing
D +86 10 5813 7038
zhisong.deng@dentons.cn

Colombia

Juanita Acosta
Partner, Bogotá
D +57 1 746 7000 ext. 266
juanita.acosta@dentons.com

Luz Helena Adarve
Partner, Bogotá
D +57 1 746 7000 ext. 232
luz.adarve@dentons.com

Czech Republic

Ladislav Smejkal
Partner, Prague
D +420 236 082 242
ladislav.smejkal@dentons.com

Dubai

Kelly Tymburski
Partner, Dubai
D +971 4 402 0997
kelly.tymburski@dentons.com

France

David Masson
Partner, Paris
D +33 1 42 68 93 54
david.masson@dentons.com

Germany

Christoph Zieger
Partner, Munich
D +49 89 2444 084 23
christoph.zieger@dentons.com

Dr. Constantin Rehaag
Partner, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

Hong Kong

Julianne Doe
Partner, Hong Kong
D +852 2533 3689
julianne.doe@dentons.com

Hungary

István Réczicza
Partner, Budapest
D +36 1 488 5200
istvan.reczicza@dentons.com

Poland

Igor Ostrowski
Partner, Warsaw
D +48 22 242 56 73
igor.ostrowski@dentons.com

Magdalena Bartosik
Counsel, Warsaw
D +48 22 242 55 23
magdalena.bartosik@dentons.com

Russia

Victor Naumov
Office Managing Partner, St.Petersburg
D +7 812 325 8444
victor.naumov@dentons.com

Singapore

Woon Chooi Yew
Senior Partner, Singapore
D +65 6885 3609
woonchooi.yew@dentons.com

South Africa

Shahid Sulaiman
Partner, Cape Town
D +27 21 686 0740
shahid.sulaiman@dentons.com

Turkey

Galip M. Selçuk
Partner, Istanbul
D +90 212 329 30 00
gselcuk@baseak.com

UK

Nick Graham
Partner, London
D +44 20 7320 6907
nick.graham@dentons.com

Martin Fanning
Partner, London
D +44 20 7320 5582
martin.fanning@dentons.com

US

Todd D. Daubert
Partner, Washington, DC
D +1 202 408 6458
todd.daubert@dentons.com

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

www.dentons.com

CSBrand-2484_GDPR_letter-CA-07 — 28/03/2018