Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

GDPR checklist

Contents

Introduction

The EU General Data Protection Regulation (**GDPR**)[1] will apply directly in all EU Member States from 25 May 2018. It will repeal and replace Directive 95/46EC and its Member State implementing legislation.

Together with the Directive on the Processing of Personal Data for the Purpose of Crime Prevention,[2] the GDPR presents the most ambitious and comprehensive changes to data protection rules around the world in the last 20 years.

The GDPR rules apply to almost all private sector processing by organisations in the EU or by organisations outside the EU which target EU residents. The export regime will ensure their impact is felt where such organisations transfer personal data to the EU. The maximum fines for non-compliance are the higher of €20m and 4% of the organisation's worldwide turnover.

The concept of accountability is at the heart of the GDPR rules: it means that organisations need to be able to demonstrate that they have analysed the GDPR's requirements in relation to their processing of personal data and that they have implemented a system or programme that allows them to achieve compliance.

This table is designed to give an illustrative overview of the requirements likely to impact most types of businesses and the practical steps that organisations need to take to meet those requirements. It can be used to gain an understanding of where an organisation has gaps in its compliance and to articulate how its control programme meets the requirements. It should be noted that certain parts of the GDPR (such as exceptions to the data subject rights) will be supplemented by Member State local legislation and guidance from local data protection authorities, which will be renamed Supervisory Authorities, and the Article 29 Working Party, which becomes the European Data Protection Board under the GDPR.

If your organisation needs assistance with analysing and implementing changes arising from the application of the GDPR please contact one of the Norton Rose Fulbright European data protection team members whose details are set out at the back of the checklist.

[1] Publication of the English text in the Official Journal can be found here http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[2] This was approved on the same date and the final English text can also be found at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Territorial scope

The scope of the GDPR is extended so that many companies based outside the EU that are processing personal data about persons who are in the EU need to comply and appoint a representative in the EU.

Arts 3, 27

Rec 22-25

Controllers outside the EEA

The GDPR applies to controllers and processors established in the EU. It also applies to non-EU establishments where data about data subjects who are in the EU is processed in connection with "offering goods or services" or "monitoring" their behaviour.

Organisations should:

- identify non-EU group companies that monitor, track or target EU data subjects.

Art 27

Rec 80

Appointing a representative for non-EU entities

Where the controller or processor is not established in the EU but is caught within the scope of the GDPR, the controller or processor must designate a representative in a Member State in which the data subjects are whose personal data is processed in relation to the offering of goods or services, or whose behaviour is monitored, unless an exception applies (e.g. where the processing is occasional or where the organisation is a public body).

Organisations should:

- consider whether such non-EU group companies need to have an EU representative or whether an exemption applies;
- ensure that where such non-EU group companies are required to have an EU representative, that the representative is appointed in an appropriate EU country, that such appointment is in writing and that the company has complied with GDPR rules in respect of that processing (including in respect of required documentation as described below).

Supervisory authority

The GDPR requires national data protection authorities (**Supervisory Authorities**) to respond to complaints and enforce the GDPR and local data protection laws where only data subjects in that member state are affected. Where there is cross border processing, a lead Supervisory Authority system (determined by the location of the "main establishment" of the organisation) applies through which that authority enforces the GDPR in consultation with the other "concerned" Supervisory Authorities.

Arts 4, 55, 56 and 60

Rec 36, 37, 124-128

Main establishment

If controllers or processors have establishments in more than one Member State, the GDPR sets out criteria for determining which of the establishments is the "main establishment" and therefore which Supervisory Authority is the lead Supervisory Authority and will enforce the GDPR in respect of cross border processing. Processing that only affects one Member State continues to be enforced by that Member State's Supervisory Authority.

Organisations should:

- determine where the organisation's "main establishment" is likely to be by considering where the central administration is, where the decisions on processing personal data are taken and where the main processing activities take place to determine if a lead Supervisory Authority will assert jurisdiction;
- design and implement policies to support aggregation or disaggregation of group liability to the main establishment through intra-group, customer and service provider agreements;
- assess the likelihood of the main establishment being deemed to be the controller of a "group of undertakings" and the associated liability issues.

Data governance and accountability

The GDPR places onerous accountability obligations on controllers and processors to demonstrate compliance with the GDPR. Some of the elements that must be demonstrated are explicit but some are implied, such as the implementation of appropriate governance models so that data protection receives an appropriate level of attention within the organisation.

Some of the requirements already exist in French or German data protection law today and some formalise what is regarded as best practice (but not legally required) under the laws of other EU Member States. The net effect is that all large organisations need to implement a formal data protection programme.

Governance – Appointment of responsible personnel and implementation of appropriate reporting lines

Implied

Art 24, 37-39

Sufficient prominence in organisation and board support

The GDPR requires organisations to implement measures to reduce the risk of non-compliance with the GDPR and to demonstrate that data protection is taken seriously. Data protection officers are required to report directly to the highest management level within the organisation. It is clear that data protection requires significant prominence within organisations as well as board attention and support.

Organisations should:

- educate their senior management about the requirements under the GDPR and the possible impact of non-compliance;
- identify key senior stakeholders to support the data protection compliance programme;
- allocate responsibility and budget for data protection compliance;
- consider reporting lines within the data protection governance structure. Supervisory Authorities expect reporting lines on data protection compliance to the board (or equivalent top management level).

Arts 37- 39

Rec 97

Appointment of a data protection officer

Whereas previously the appointment of a data protection officer (a **DPO**) was optional in most Member States, controllers and processors are now *obliged* to appoint a DPO in certain circumstances, including: (a) where the core activities of the organisation consist of processing operations which require "*regular and systematic monitoring*" of data subjects on "*a large scale*"; or (b) where the core activities consist of processing of special categories of data on a "*large scale*"; or (c) where required under Member State law (where lower thresholds apply).

The DPO should report to the highest management level of the controller or processor (as appropriate) and must be supported in carrying out its functions, including with the necessary resources.

The DPO's contact details must be notified to the Supervisory Authority so that he/she will be the first official contact point on any issues.

Organisations should:

- consider whether they *have* to appoint a DPO and, if not, whether they still wish to;
- if they have more than one establishment, consider whether a single DPO would be easily accessible from each establishment and would therefore suffice or whether more than one DPO is required;
- be clear as to whether the person they have given responsibility to is a formal DPO (with the relevant protections in the GDPR, e.g. around dismissal, independence and instructions) or not and whether his/her advice would ever be subject to legal privilege;
- consider their staffing structure to ensure that the DPO reports to the highest management level and is involved in a timely manner in all issues which relate to the protection of personal data;
- if the DPO carries out other tasks and duties, consider how they ensure that the DPO does not become subject to a conflict of interest;
- consider how they will support the DPO with the necessary resources (e.g. staffing resources, board support, budget);
- publish the DPO's contact details and notify the relevant Supervisory Authorities of the same.

Art 39

Training

DPOs are under a specific obligation to implement appropriate training. Although not an express obligation for organisations where DPOs are not required, we consider it to be almost impossible to demonstrate that an organisation is able to achieve compliance without policies setting out how to comply coupled with training to bring those policies to life.

Organisations should:

- implement a training programme covering data protection generally and the areas that are specifically relevant to their organisations;
- implement a policy for determining when training should take place and when refresher training should be carried out as well as a process for recording when training has been completed.

Privacy by design and privacy impact assessments

Art 25

Rec 74, 78, 83

Privacy by design

Controllers should take steps to show that they have taken data protection compliance into consideration, and have implemented appropriate compliance measures in relation to their data processing activities. In particular, controllers should adopt internal policies and measures which meet the principles of privacy by design and data protection by default.

Organisations should adopt internal policies and implement technical and organisational measures:

- relating to pseudonymisation, the use of cryptographic procedures for the protection against unauthorised or unlawful processing by both external and internal "attackers" data subject transparency and access;
- which provide that only personal data which is necessary for each specific purpose of the processing is processed (in particular in relation to the amount of data collected, the extent of its processing, the period of its storage and its accessibility);
- which provide that personal data is not made accessible to more individuals than necessary for the purpose, using applications or processes which allow them to implement such controls and (where available) have been certified by a body accredited by a Supervisory Authority which may become a way of demonstrating compliance with the privacy by design requirements.

Art 35

Rec 84, Rec 89-95

Privacy impact assessments (PIAs)

The GDPR now formalises the requirement to carry out privacy impact assessments (**PIAs**) in certain circumstances. Specifically, controllers must carry out privacy impact assessments where a type of processing is likely to result in a high risk for the rights and freedoms of individuals.

The GDPR gives some examples of where PIAs are required (e.g. in the event of a systematic monitoring of a publicly accessible area or in the context of profiling on which decisions are based that produce legal effects). It also contemplates Supervisory Authorities publishing further guidance and examples of when PIAs ought to be carried out and where they are not necessary.

Organisations should:

- have in place a process for determining whether a PIA is required;
- if they come to the conclusion that no PIA is required, document this decision properly;
- if it is determined that a PIA is required, ensure that there is a clear process for ensuring that PIAs are carried out appropriately across the organisation and include the minimum requirements, namely:
  - a systematic description of the processing operations and purposes of the processing;
  - an assessment of the necessity and proportionality of the processing operations;
  - an assessment of the risks to the rights and freedoms of data subjects (if appropriate, organisations should seek the views of the affected data subjects. This may involve consulting works councils or similar representative bodies);
  - measures envisaged to address the risks.

Art 36

Rec 84

Processing requiring approval of Supervisory Authority

If a PIA indicates that processing would result in a high level of risk in the absence of measures taken by the controller to mitigate the risk, the controller must consult the Supervisory Authority prior to the processing.

Organisations should:

- ensure that their PIA process clarifies when the results of a PIA should be referred to a Supervisory Authority and also how frequently the processing of personal data should be reviewed, to ensure that it is performed in compliance with the PIA. Such a review should be carried out at the very least where there is a change to the risks posed by the processing operations.

Accountability and demonstrating compliance

Art 7, 8

Rec 42

Demonstrating consent

A controller must be able to demonstrate that consent was given when relying on consent as a ground for processing personal data.

Organisations should:

- consider how they record consent and consider how to keep a clear record of what each individual data subject consented to;
- consider how to obtain parental consent where offering information society services to children under 16 (or such lower threshold age provided by the relevant Member State law).

Arts 5, 24, 26, 28, 32, 33 and 34

Rec 74, 77, 78, 84-86

Demonstrate compliance with GDPR

A controller must be able to *demonstrate* compliance with the data protection principles in Article 5.

A controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR, including through the use of appropriate data protection policies.

Organisations should:

- map their current processing activities (and populate an internal data processing register (see below));
- consider whether they are compliant with the provisions of the GDPR, including the data protection principles in Article 5, by working through a version of a checklist similar to this one and recording whether the requirements are applicable and where they are, how they are met (including through cross referencing policies, controls and training measures);
- review or put in place internal data protection policies / guidelines covering at least the following areas:

Employee data

  - HR department handling of employee data
  - a notice provided to employees of all data collected and for what purpose (both employee, customer and other third parties)
  - general handling of other employees' personal data and customer personal data by all employees
  - monitoring of employee communication and internet usage (including through BYOD solutions and social media)
  - accessing employee files / communications for investigations
  - use of CCTV
  - operation of whistleblowing scheme
  - any additional rules that apply in Member States

Customer data

- external privacy policy
- customer marketing protocols and consents
- cookies and online tracking and consent mechanism

Other third party data

- supplier / business partner notices / consents

Data transfers to third parties

- data sharing with other controllers (with safeguards against joint controller shared liability position)
- data sharing with processors (updated to take account of the new processor liability position)

Data subject rights

- responding to data subject rights, i.e. subject access, rectification, erasure, restriction of processing, data portability, right to object to certain types of processing and right to object to or obtain human intervention in certain automated decision making

Privacy by design and PIAs

- privacy by design / privacy by default guidance principles
- PIA triage procedures and PIA templates
- procedures to use PIAs or other documented assessments to demonstrate that new processing or technologies have been considered against the GDPR and how they meet the requirements

Information security

- information security (based on the risks to data subjects) and data breach response policy

Data storage periods

- records management programme which has been adapted so that there are maximum storage periods for personal data categories as well as minimum retention periods

Art 30

Rec 82

Internal data processing register for controllers

Controllers (and the controller's representative if the controller is outside the EU) must maintain a formal, written record of processing activities under its responsibility. Whilst controllers are currently required to provide much of this information when they register with a Supervisory Authority, the information required under Article 30 is more detailed than the requirements in some Member States.

The requirement does not apply where the controller employs fewer than 250 persons and the processing is not likely to result in a risk for the rights and freedoms of data subjects, is not occasional, or is not of special categories of data (which means most organisations will be caught as most organisations process some special categories of personal data in relation to their employees).

Controllers should:

- clearly identify where personal data is processed within their organisation, including by third party processors;
- draft a register to record details of:
  - the name and contact details of the controller and any joint controller, the controller's representative and the DPO;
  - the purpose of the processing;
  - a description of categories of data subjects and personal data;
  - the categories of recipients of personal data;
  - the details of transfers to third countries;
  - the time limits for erasure of different categories of data (possibly by cross reference to the records management programme);
  - a general description of technical and organisational security measures taken (possibly by reference to the information security policy and information classification policy);
- consider how they will ensure that the relevant information will be kept up-to-date. This may require allocating responsibility for this to individuals within the different business functions that process personal data.

Art 30

Rec 82

Internal data processing register for processors

Processors must now maintain a record of all categories of personal data processing activities carried out on behalf of a controller.

Processors should:

- determine the process they will use to record the following details in respect of each controller:
  - name and contact details of the processor and the DPO, and of the controller on behalf of which it is processing;
  - categories of processing;
  - transfers of data to a third country or international organisation;
  - general description of the technical and organisational security measures;
- consider how they will ensure that the relevant information will be kept up-to-date.

Works councils

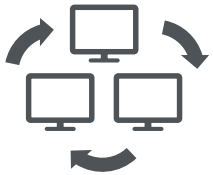
No specific new requirement

Consultation with works councils

Although the GDPR does not impose additional requirements in respect of liaising with works councils, where changes are made to the way employees' data is processed, there may be consultation rights and obligations to obtain prior consent from the works councils where these have been established.

Organisations should:

- consider in which countries they have established works councils and what agreements are currently in place with their works councils;
- review GDPR required changes to data processing operations, notices, policies and procedures and consider which of these require works councils' prior consent or consultation.



Export of personal data

The shape of export restrictions remain similar under the GDPR with some streamlining.

Arts 44-50

Rec 101-116

Whilst some of the administrative burden has been reduced because transfers based on approved mechanisms no longer have to be notified to or approved by Supervisory Authorities, the basic principles of the export regime remain similar to the existing framework.

Key differences are that:

- processors are directly required to comply with the export provisions;
- binding corporate rules (**BCRs**) and processor binding corporate rules (**PBCRs**) and the related approval process (which has been simplified) are hard-wired into the GDPR;
- sectors in a third country (e.g. the healthcare or financial services sector) can be found adequate by the Commission if they meet the adequacy requirements;
- the rules for third country and sector adequacy findings (white listing) reflect the Schrems ruling and must be reviewed at least every 4 years;
- Supervisory Authority or Commission approved codes of conduct or certification mechanisms which cover the importing entity and provide third party rights to data subjects may be recognised as an approved export solution;
- Commission approved standard contractual clauses, codes of conduct / certifications (which meet the requirements in the previous paragraph) and approved binding corporate rules (and PBCRs) can be used to legitimise export without further approvals from Supervisory Authorities.

Organisations should:

- review and map their international data flows, including:
  - intra-group data flows;
  - extra-group data flows where a EEA group company controller is exporting to a controller or processor outside of the EEA;
  - extra-group data flows where a non-EEA group company is importing as a processor or controller;
  - consider what existing data transfer mechanisms are in place and whether these continue to be appropriate. Countries that are currently white listed remain so until a Commission review finds otherwise (Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay and New Zealand);
  - consider whether BCRs or PBCRs would be a viable option for intra-group data transfers;
  - consider putting in place a process for responding to requests for information from non-EEA litigants, regulators or law enforcement agencies and ensure that relevant staff are made aware of such a process;
- ensure that export obligations are flowed down through subcontractor chains and across to other controllers where required.

- the grounds for transfer to a non-EU court or administrative authority appear to have become stricter requiring an international agreement, such as a mutual legal assistance treaty, between the requesting third country and the European Union or the relevant member state (although this area is complex and the drafting is unclear);
- failure to comply with the export rules can attract the highest 4% of worldwide turnover fines.

Joint controllers

The GDPR further articulates how responsibility / liability should be apportioned between joint controllers.

Arts 26 and 82

Rec 79, 82

Joint controllers

In circumstances where two or more parties determine the purposes for which and the manner in which the personal data is processed, each party will be a controller and will be liable for the entirety of any damage to a data subject, unless they can prove they were not in any way responsible for the event giving rise to the damage.

Organisations should:

- consider whether there are any intra-group, customer or service provider arrangements where a group company is a joint controller;
- ensure that there is a clear attribution of data protection responsibilities between joint controllers and that this information is made available to data subjects through privacy notices or other means so that a controller is able to show it was in no way responsible for the event giving rise to the damage if this is the case;
- ensure that contract negotiators are aware of the default position of each controller being liable for the entire damage to a data subject if it is in any way responsible for the event giving rise to the damage and include appropriate cross indemnification.

Processors

Processors now have direct obligations under the GDPR and can be liable to fines from Supervisory Authorities and claims from data subjects.

Arts 28, 37, 82 and 83

Rec 81

Processors

Processors have direct obligations to implement technical and organisational measures including: not to appoint sub-processors without (i) the consent of the controller and (ii) flowing down the same provisions; to notify breaches to the controller; and to cooperate directly with the Supervisory Authority.

The minimum requirements to be set out in processor agreements are more extensive than legally required in most Member States today.

If processors breach their direct obligations they can be fined by the Supervisory Authorities and held jointly liable with the controller for the entirety of any damage to a data subject, unless they can prove they were not in any way responsible for the event giving rise to the damage.

Organisations should:

- assess any intra-group processor agreements and make amendments to include minimum requirements and if necessary to keep liability limited towards the group's main establishment or service companies;
- amend extra-group agreements where a group company is a processor to provide for the new liability position;
- amend extra-group agreements where a group company appoints a processor to include minimum required terms.

Lawful grounds to process and consent

The GDPR includes new limitations on the use of consent as a ground for processing and provides some examples as to what constitutes legitimate interest grounds for processing. The duties to supply information to data subjects also require processing grounds to be determined and articulated.

Arts 6-10

Rec 32, 42-49

Lawful grounds to process and consent

The GDPR requires the identification and articulation of the grounds for lawful processing and the storage period for the data in fair processing notices (see next section).

The rules around consent are more onerous and consent must be as easy to withdraw as to give.

Certain purposes such as intra-group transfers and direct marketing are specified as legitimate interests in the recitals.

Organisations should:

- in relation to each type or category of processing, ensure that they have identified and documented the grounds for lawful processing (and where the legitimate interests ground is being used, what the legitimate interests are) and the storage period for the data (required for the fair processing notice, see next section). This information could be included in the internal data protection register;
- given the new limitations around consent, ensure that consent is used as a ground only where it is the only way to justify that processing;
- where processing relies on consent and consent is made a condition of receipt of a service, either document the justification (e.g. that it is necessary for the performance of the contract) or document a sufficient incentive to justify such conditionality (e.g. that a cheaper service is being provided in exchange for the consent);
- redraft forms which rely on consent so that:
  - they reflect the previous two bullets;
  - each purpose is consented to separately unless it is appropriate to bundle the purposes;
  - it is made clear that consent may be withdrawn (and that there is an easy mechanism through which this can be effected (e.g. a self-service dashboard));

- put in place procedures to deal with evidencing that consent has been obtained and any withdrawals of consent, and consider the impact of withdrawal on the underlying processing;
- where consent is obtained from children under 16[3], ensure that a mechanism to obtain consent from a parent is built into the consent mechanism;
- ensure that if criminal convictions or offences data is processed, the organisation complies with any Member State requirements;
- consider whether any additional provisions under Member State law relating to grounds for processing personal data may apply (e.g. compliance with a legal obligation or in relation to the processing of sensitive personal data).

[3] This may be as low as age 13 where this is provided for under local Member State law.

PRIVACY POLICY

Fair processing information / notices

The GDPR extends the information that is required to be given to data subjects.

Arts 12 – 14

Rec 58-62

Fair Processing Notices

The information that is required to be given to data subjects is extended to include: providing details of the grounds that are used to justify processing (including the legitimate interest relied upon if that ground is being used) and the period for which the personal data will be retained (or at least the criteria for determining the storage period); if exported the export solution and means to obtain a copy of the solution; the source of the data (if not the data subject him / herself) and whether obtained from a public source; and in certain circumstances more information on wholly automated processing.

The notice must highlight that consent may be withdrawn, the existence of the data subject rights set out below and the right to lodge a complaint with the Supervisory Authority.

Finally, the notice must be given in a concise, transparent, intelligible and easily accessible form using clear and plain language. Icons may be used. Where presented electronically the information conveyed by the icons must be machine readable.

Organisations should:

- consider the best process to provide such information in a clear and intelligible form, including how to make the information machine readable;
- update employee notices to take account of the new requirements;
- update customer notices to take account of the new requirements;
- where group companies are obliged to provide notice on behalf of a third party, ensure that notices have been updated (and necessary information obtained from the third party to do so);
- where a third party is obliged to provide notice on behalf of a group company, ensure that the third party has been given the necessary information to put in the notice and a deadline imposed by which the notice must be updated and given;
- consider any other circumstances where data processed by a group company has not been provided to the company by the data subject themselves and how information notices may be provided to the data subjects.

Data subject rights

Data subject rights have been significantly enhanced under the GDPR including a new right of data portability and an enhanced right of erasure. The information to be provided pursuant to a data subject access request has also been increased.

Arts 12, 15-23

Rec 63-73

Data subject rights

Data subject rights are enhanced to include rights:

- to have personal data transmitted to the data subject or another controller in a commonly used machine readable format (data portability);
- to require the controller to erase personal data in certain circumstances and where the data has been made public to take reasonable steps to inform controllers that are processing the data that the data subject has requested its erasure of any links to, copies or replication of it (right to be forgotten);
- to more information about a controller's processing (export solution, storage limits) through a subject access request and to provide the information in a commonly used electronic form;
- to require data to be marked as restricted whilst complaints are resolved.

Action must be taken by controllers within 1 month of, or if complex within 3 months of, a request.

Some exceptions to the rights are in the GDPR. The majority are set at a high level by the GDPR but are to be detailed by Member State legislation.

Organisations should:

- assess how these rights trigger and how they will be exercised in both customer and employee contexts;
- consider how to search for, filter and separate the information required to comply with the rights;
- consider whether the rights can be met wholly or partially through a self-service option;
- identify the relevant exemptions under Member State law (e.g. in areas of national security, defence, prevention / detection of crimes, public security or public interest) and how the rights can be resisted where desirable;
- ensure that mechanisms are in place to enable responses within one month;
- assess the opportunities to have personal data of competitors or other third parties' customers ported to the organisation through data subject's exercise of portability rights.

Big Data, research and wholly automated decision making

The rules in relation to Big Data and research have not changed very significantly.

Arts 6, 9, 21, 22, 89

Recs 50, 65, 71, 91, 156-163

Big Data, research and wholly automated decision making

The framework for secondary use of personal data is very similar to the existing position.

The framework for wholly automated decision making is very similar to the existing position but additional factors can trigger the threshold condition (location, movements, health, personal preferences and interests of the data subject) and use of sensitive personal data is prohibited without explicit consent or unless authorised by EU or Member State law.

The framework for processing for scientific, statistical or historical purposes is presumed to be compatible with original purposes, subject to any additional Member State and EU legislative safeguards. So research regimes will remain at the Member State level.

Organisations should:

- where data is used for a secondary purpose beyond scientific, statistical, historical purposes, ensure that the use is in compliance with the current Article 29 WP203 test for secondary uses (a conservative balancing test) such that:
  - the link between original and secondary purposes is assessed;
  - the context and relationship between the data subject and controller have been considered;
  - the nature of the personal data has been considered;
  - the possible consequences of the processing has been considered;
  - safeguards (functional separation / encryption / pseudonymisation) are put in place;
- consider whether a data protection impact assessment should be undertaken;
- implement appropriate consent mechanisms and the ability to re-evaluate the decision by human means for wholly automated processing where the threshold conditions are passed or sensitive personal data is processed and the evaluation to enter into, or performance of a contract or authorised by law exemption is not available;
- ensure that bias in decision making is understood and that safeguards are implemented to counter against it;
- identify and comply with specific Member State scientific, statistical or historical research rules.

Personal data breach

The GDPR introduces new timeframes for notifying Supervisory Authorities and data subjects and requirements regarding the details that are required to be recorded and provided in such circumstances.

Art 33, 34

Rec 85-88

Personal data breach response

The new breach notification law provides for a 72 hour deadline in respect of notifications to the relevant Supervisory Authority and a requirement to provide notifications to data subjects "without undue delay" in certain high risk circumstances.

They also require the controller to maintain a personal data breach register.

Organisations should:

- put in place data breach response and notification procedures to meet 72 hour deadlines in respect of notifications to the Supervisory Authority;
- put in place data breach response procedures to evaluate situations exposing data subjects to high risk and procedures to enable notifications to be made to data subjects "without undue delay" in such circumstances;
- prepare template letters and conduct rehearsals in respect of data breaches;
- maintain a personal data breach register, including at least the facts relating to the breach, the impact and the remedial actions taken;
- ensure that processor agreements have provisions allowing group company controllers to meet the 72 hour deadlines for reporting breaches to the Supervisory Authority and that the liability position is understood;
- ensure that where a group company is a processor, that mechanisms are in place to enable it to report data breaches without undue delay to the controller;
- review insurance coverage for data breaches and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR and increased likelihood of complaint / action by data subjects.

Notes

General Data Protection Regulation text used – 6 April 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

GDPR Application Date means the date from which the GDPR applies (25 May 2018)

The team

EMEA

Marcus Evans
Partner, London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Rohan Isaacs
Partner, Johannesburg
+27 11 685 8871
rohan.isaacs@nortonrosefulbright.com

Pietro Altomani
Senior Associate, Milan
+39 02 86359 476
pietro.altomani@nortonrosefulbright.com

Christoph Ritzer
Partner, Frankfurt
Tel +49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Adjou Ait Ben Idir
Partner, Dubai
+971 4 369 6393
adjou.aitbenidir@nortonrosefulbright.com

Agnieszka Braciszewska
Senior Associate, Warsaw
+48 664 549 499
agnieszka.braciszewska@nortonrosefulbright.com

Nadège Martin
Partner, Paris
+33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

Attilio Pavone
Partner, Milan
+39 02 86359 417
attilio.pavone@nortonrosefulbright.com

Nikos Anagnostopoulos-Gioussas
Senior Associate, Athens
+30 210 94 75 410
nikos.anagnostopoulos@nortonrosefulbright.com

Jamie Nowak
Partner, Munich
Tel +49 89 212148 305
jamie.nowak@nortonrosefulbright.com

Jurriaan Jansen
Of Counsel, Amsterdam
+31 20 462 9381
jurriaan.jansen@nortonrosefulbright.com

Kerri Crawford
Senior Associate, Johannesburg
+27 11 685 8929
kerri.crawford@nortonrosefulbright.com

Maartje Govaert
Partner, Amsterdam
+31 20 462 9329
maartje.govaert@nortonrosefulbright.com

Lara White
Senior Associate, London
Tel +44 20 7444 5158
lara.white@nortonrosefulbright.com

APAC

Stella Cramer
Partner, Singapore
+65 6309 5349
stella.cramer@nortonrosefulbright.com

Anna Gamvros
Partner, Hong Kong
+852 3405 2428
anna.gamvros@nortonrosefulbright.com

Barbara Li
Partner, Beijing
+86 10 65353130
barbara.li@nortonrosefulbright.com

Nick Abrahams
Partner, Sydney
+ 61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Jim Lennon
Special Counsel, Sydney
+ 61 2 9330 8426
jim.lenon@nortonrosefulbright.com

US

David Kessler
Partner, New York
Tel +1 212 318 3382
david.kessler@nortonrosefulbright.com

Andrea L. D'Ambra
Partner, New York
Tel +1 212 318 3015
andrea.dambra@nortonrosefulbright.com

Kim Gold
Senior Counsel, New York
+1 212 318 3103
kim.gold@nortonrosefulbright.com

Canada

Julie Himo
Partner, Montreal
+ 1 514 847 6017
julie.himo@nortonrosefulbright.com

Caroline Deschenes
Associate, Montreal
+ 1 514 847 6071
caroline.deschenes@nortonrosefulbright.com

APAC

Stella Cramer
Partner. Singapore
+65 6309 5349
stella.cramer@nortonrosefulbright.com

US

Canada

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.