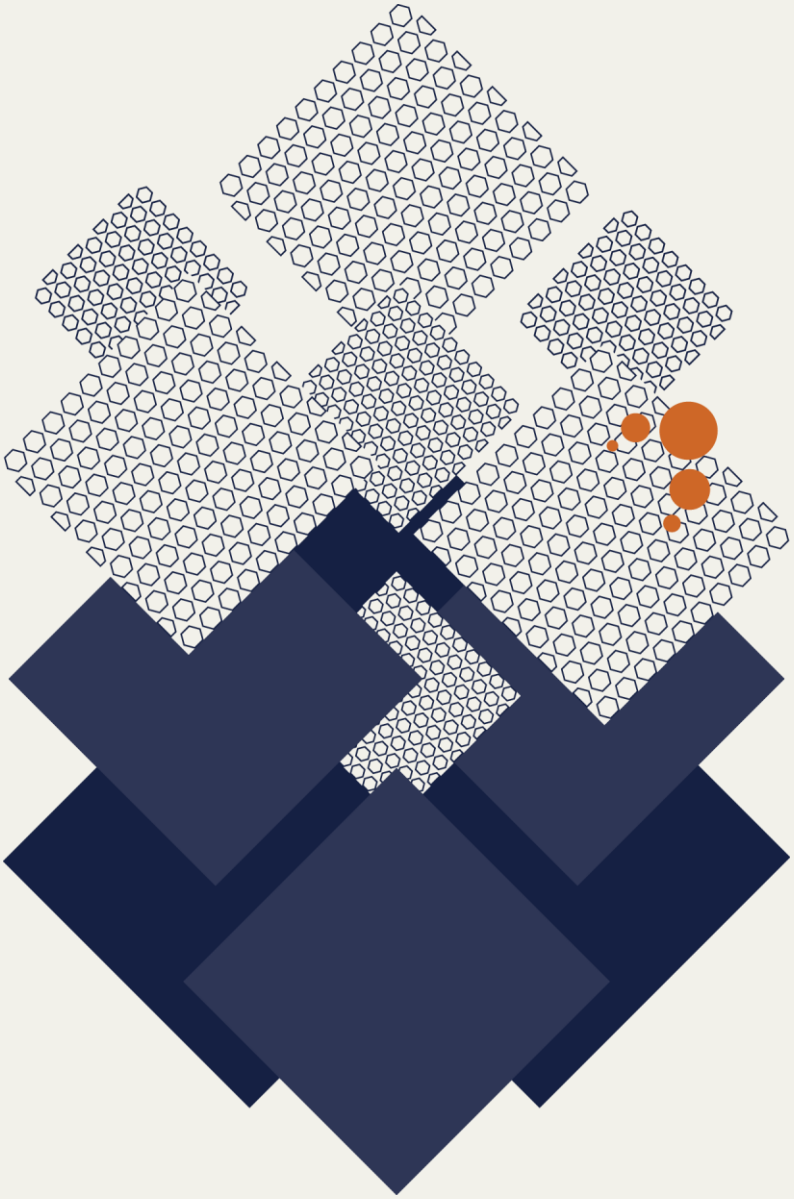
Noerr



General Data Protection Regulation

Key News

/ Introduction

The General Data Protection Regulation[1] ("**GDPR**") was approved on 27 April 2016 and is set to come into force on 25 May 2018. It will replace the current national legislations on data protection and the EU Data Protection Directive of 1995[2] ("**Directive**") on the protection of individuals with regard to the processing of personal data and the free movement of such data. In order to provide consistent and homogenous rules for personal data protection, the GDPR will be directly applicable. This means that Member States do not have to transpose the Regulation into their own legislation.

The declared objective of the GDPR is to achieve a high level of protection of the rights of EU citizens against unauthorised use of their data and personal data. The GDPR affects all companies, individuals or other institutions which process users' data. As a result, it is necessary for all those concerned to review their information systems and the ways they treat personal data.

The GDPR emphasises the responsibility of the controller to adhere to the Regulation and encourages those handling data to adopt internal measures that will enable them, as controllers, to prove compliance. In particular, it is necessary to adapt internal mechanisms for data processing in such a way that the controller is able to provide data subjects with transparent, easily accessible and intelligible information. Increased administrative burdens can be expected in connection with this duty, as the controller will among other things have to document that it only processes data which is necessary for the particular purpose.

The GDPR also brings a number of new rights for data subjects. Above all, data subjects will have to be informed in detail of their rights. The possibility of the subjects concerned to raise an objection to the processing of their personal data is new. In practical terms, if the controller does not have compelling legitimate grounds for keeping particular data, it cannot continue processing such data. The subject must be able to access the data collected on them at any time. Data subjects also have the right to data portability. This creates the obligation for the controller to issue a copy of the subject's data in a machine-readable format so that they are able to convert it into another system for further use. New is the "right to be forgotten". This enables data subjects to request that the controller erases the data and refrains from continuing to store and disseminate it if it is no longer necessary in relation to the purposes for which it was collected.

---

[1] REGULATION (EU) No. 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Directive (EU) No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The controller is obliged to keep records about all processing activities. The controller must be ready to submit these records to the supervisory authority at any time.

The GDPR not only adds new rights and obligations, but also expands the definition of personal data. Technical parameters such as e-mail addresses and IP addresses are now expressly covered. A very important part of the GDPR is the notification obligation in the event of a personal data security breach. The controller will now have to notify the supervisory authority of any personal data leak within 72 hours of becoming aware of it.

/ Table of Contents

/ Data protection officer ("DPO")

The GDPR also introduces the position of data protection officer ("**DPO**") on a pan-European level. While some European countries are already familiar with this institute, the position is completely new in most of the national environments. According to the Regulation, the data protection officer should function as a coordinator of personal data protection for the particular controller or processor, and at the same time represents a contact point for communication with supervisory authorities.

The obligation to appoint a DPO arises in three cases. One of them is situations where data processing is carried out by a public authority or body, except for courts. Another is where the controller's activities consist of operations which require large and systematic monitoring of citizens. And finally, situations where the core activities of the controller or processor consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offences.

The DPO can be an employee of the controller or processor or he/she can perform his or her tasks on the basis of a service contract (i.e. externally). The name and contact details of the data protection officer are subsequently communicated to the regulator and the public. It is necessary to ensure that this person is personally available (physically or by secure means of communication). When carrying out his/her activities, the DPO is bound by the duty of confidentiality.

One of the data protection officer's main tasks is to check whether the internal practices of a company comply with legislation dealing with personal data protection. The DPO is required to collect information to recognise and identify the processing of personal data and to subsequently inform, advise and provide recommendations to the personal data controller or processor.

It is advisable for controllers and processors to seriously consider whether they are obliged to appoint a data protection officer to protect personal details and, if not, whether it is appropriate to create this position voluntarily. By appointing a DPO the controllers and processors to whom the GDPR applies do not relieve themselves of their responsibility to provide protection for personal data. Nevertheless, appointing one can make it easier to ensure that obligations arising from personal data protection are met. In the case of a breach it can alleviate responsibility by indicating that the controller or processor has made all possible efforts to protect personal data.

/ Profiling

The GDPR contains a special rule on profiling which will significantly affect many personal data controllers. Nowadays, profiling and analysing large amounts of data play a key role in the growth of the digital economy.

Profiling, according to the definition in Article 4 paragraph 4, means any form of **automated** processing of personal data consisting of the use of personal data to evaluate or predict aspects concerning that natural person's behaviour. Such forms of profiling include, for example, evaluation of a person's work performance, evaluation of their economic situation for the purpose of offering a suitable financial or insurance product, their state of health, personal preferences, interests, location or movements.

Currently, entrepreneurs collect extensive information on data subjects to offer products or services directly custom-made for the customer. Profiling has become a common part of e-shops, marketing and other fields. These fields will be greatly influenced by the new GDPR and profiling.

The GDPR does not contain a definition of automated processing. A certain guideline can be found in Council of Europe Convention No. 108, which defines automated processing as the process of an operation or operations carried out in whole or in part by automated means: storage of data, carrying out logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination. This makes it clear that the automated processing of personal data takes place when automated procedures or means are used for processing personal data.

The issue of profiling, based on which automated individual decisions are made, is significant for the controller because of the obligations arising from the GDPR if such profiling is carried out. The definition of automated individual decision-making can be found in Article 22 of the GDPR, which states that it is "*decision-making or decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".

One of the basic obligations resulting from the GDPR for the controller or processor is the information obligation. The data subject must be informed of the fact that his or her data is profiled. The information given must define the purpose, meaningful information concerning the procedure used, as well as the meaning and envisaged consequences of such processing for the data subject.

Another right of data-profiling subjects is the possibility to be removed from profiling. The subject has the right not to be included in profiling if it is carried out by automated means. He or she must be removed as soon as they raise an objection or withdraw their consent. Article 21 of the GDPR deals with the possibility to raise an objection and states that if a data subject exercises his/her right and raises an objection to such processing, the controller must immediate cease processing the personal data, i.e. may no longer process it, unless the controller

demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The issue of profiling is extensive and it is likely that it will have a significant impact on companies that take part in carrying out automated data processing for profiling purposes. It is important that such companies analyse processes which lead to the processing of personal data based on profiling and adapt them to the new conditions set out in the GDPR.

/ Right to portability

The GDPR will establish a brand new right of data subjects called the "right to portability". This new right is related to the right of access already enshrined in the Directive. However, it also significantly differs from the above right. Whilst the right of access entitles the data subject to obtain a confirmation from the controller as to whether or not his/her personal data is being processed and plus the right to access this personal data, the newly established right to portability goes further and on one hand reinforces the control of data subject over his personal data, and on the other enables easy and direct transmission of the personal data from one controller to another free of charge at the data subject's request. The purpose of the new right is to improve and accelerate the functioning of the digital single market by making it easier for customers to switch between different service providers.

The right to portability of personal data consists of **two partial rights**:

1. The right of a data subject **to receive back** (from the data controller) **his/her personal** data, whereby this personal data must be in a structured, commonly used and machine-readable format, and
2. The right of a data subject **to directly transmit this data** from one data controller to another without any hindrance.

Even though the new right to portability clearly strengthens the position of data subjects, the application of the right is not unrestrained. The data subjects may only make use of the right if the conditions regarding the type of personal data, legal basis and the method of processing the data are met.

The right to portability may only apply when the **personal data relates to the data subject** who wants to make use of the right to portability. Therefore, any personal data originally related to the data subject but subsequently made anonymous will not fall under the scope of the right to portability. In many circumstances, data controllers will process information containing personal data of several data subjects. As an example, telephone records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests.

Furthermore, the right to portability may only apply when the personal data concerned was **provided to a data controller by the data subject**. However, this condition is to be interpreted more broadly than may appear at first sight. The following categories can be qualified as "provided by the data subject":

1. *Data actively and knowingly provided* by the data subject to a data controller (e.g. mailing address, user name, age, etc.),
2. *"Observed data" provided by the data subject by virtue of use of the service or the device* (including for instance a person's search history, traffic data and location data. In contrast, inferred data and derived data are out of scope.

The data which arises as an outcome of the subsequent analysis of provided personal data (derived data) is created by the data controller on the basis of the data "provided by the data subject". Therefore such data (e.g. a credit score, algorithmic results or the outcome of an assessment regarding the health of a user) is also not covered by the right to portability.

If the abovementioned conditions are met, it is irrelevant with regard to the right of portability whether the personal data concerned is categorised as so-called "*common*" personal data (such as name, date of birth, birth number) or as a "*special category*" of personal data (such as political opinions, religious beliefs, data concerning health, sex life or sexual orientation).

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data in every case. From all possible legal bases for personal data processing, the right to portability may only apply when the **legal grounds are based either on a data subject's consent** or on a **contract to which the data subject is party** and at the same time the personal data was processed **by automated means**.

Under this general condition, the exercise of the right to portability may not adversely affect the rights and freedoms of others. One example would be a situation where a data subject exercises their right to data portability over their bank account, since it can contain personal data relating to the purchases and transactions by the account holder as well as information relating to transactions that has been provided by other individuals who have transferred money to the account holder.

In this context, the rights and freedoms of the third parties are unlikely to be adversely affected in the bank account history transmission if their data is used for the same purpose in each processing, i.e. as a contact address only used by the data subject or as a history of one of the data subject's bank accounts.

Conversely, the rights and freedoms of third parties will not be respected if the new data controller uses the contact directory for the marketing purposes, for example.

If a data controller (often a company) receives the portability request from the data subject (often a customer), it is necessary to know that the request must be processed and answered without undue delay but no later than within one month, or within a maximum of three months for complex cases. Within the same periods data controllers who refuse to answer a portability request have to indicate to the data subject the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority.

The recommended technical tool for data controllers in order to answer the portability requests of data subjects for rendering back the provided personal data is **establishing of a direct download opportunity for the data subject**. In practice this could for example be implemented by making (customers) an Application Programming Interface available for the data subjects.

When making use of the part of right to portability consisting of **data transmission the data subjects may make use of a personal data store – a trusted third party holding and storing the personal data**. The data subjects may subsequently only grant permission to re-

spective data controllers to access and process the personal data as required, so data can be easily transferred from one controller to another.

/ Privacy by default

Privacy by default is one of the core principles under the GDPR next to the principle of privacy by design. Therefore, it is crucial for companies, in particular from the new technologies sector, to comply with this rule and implement it in their products and services.

In short, privacy by default means initial (basic) privacy settings of products and services (e.g. IT systems, software or online platforms) which ensure the broadest level of data protection and collection only of such data which is necessary for basic use of products or services as expected by the users. Any change in such strict privacy settings may only take place at the user's explicit choice. Privacy by default is intended to protect users from unconscious sharing of their data, in particular while using social media services.

Privacy by default is set out in Article 25 paragraph 2 of the GDPR and states that a controller is required to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. This limitation applies to the following aspects: (i) the amount of personal data collected, (ii) the extent of its processing, (iii) the period of its storage and (iv) its accessibility. In particular, such measures are designed to ensure that by default personal data is not made accessible to an indefinite number of people.

In practice, privacy by default means that by default no data should be collected and/or further processed unless it is necessary/justified. Users of products or services should always have the choice to allow use of their data in a broader way than a simple use of certain products or services. The companies should design their products or services in such a way that a user have an "opt-in" option. Furthermore, users must be informed about all privacy implications (defaults and options) when they register with a product or service and agree to change the default privacy settings later. Such information should be easily accessible on a website, clear and easy to understand. Also, users should be able to conveniently access, check and change their own privacy settings at any time.

This principle relates closely to other GDPR's principles, namely to the principles of data minimisation and purpose limitation. Personal data must be adequate, relevant and limited to data which is necessary in relation to the intended purposes in all cases. The companies cannot collect any data just in case they may need them in the future for the same purpose or a different one. Also, they can store the collected data only for such amount of time which is necessary to provide the particular product or service.

The GDPR does not provide for any list of specific technical and organisational measures in order to ensure privacy by default. It indicates only the following examples to demonstrate compliance with this rule and the GDPR as such. According to the recitals of the GDPR such measures could consist of:

- pseudonymising personal data as soon as possible,
- transparency with regard to the functions and processing of personal data,

- enabling the user to monitor the data processing,
- enabling the controller to create and improve security features.

Under the GDPR pseudonymisation is a technique for processing personal data in such a way that it can no longer be attributed to a specific person without the use of additional information which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

It will be crucial for the companies to evaluate and, if necessary, re-design their privacy settings if they currently collect data from their users in a broader way than strictly necessary for a particular purpose. Moreover, if they want to share a user's data with any third parties they need to request the user's consent in a first step.

The privacy by design principle will be especially visible in social media services when a user creates a profile and shares data with others. Such profiles may only show non-users or other users very limited information by default and any other data may only be accessible with the explicit consent of the user. Moreover, privacy by default will be applied in Internet browser's settings. The browser's default settings must ensure the possibility to give free and conscious consent for profiled advertising.

/ Data protection by design

The current Directive has no equivalent to the concept of privacy by design. Privacy by design or data protection by design is the notion that the means and purposes of personal data processing are designed, from the beginning, with data protection in mind.

The present system of various national laws which transposed the Directive resulted in a fragmented regulatory system for data controllers operating in the European Union. It often happened that a multinational company operating in different countries in the EU had to use several versions of their data protection policies in order to comply with the national laws. It meant different documentation requirements, different software to use and different methods for storing, deleting or forwarding data for each and every country within the same company. In the GDPR a more standardised data protection law will come into force across the EU.

The GDPR addresses the principle of data protection by design as a legal obligation for data controllers and processors for the first time, making explicit reference to data minimisation and the possible use of pseudonymisation. Data minimisation means that personal data must be adequate, relevant and limited to data which is necessary in relation to the purposes for which it is processed. Pseudonymisation refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

This principle – together with the principle of data protection by default – encourages controllers and processors to include data protection measures from the start of the process, at the design stage of their products and services. The principle requires organisations to implement both technical and organisational measures that will guarantee and protect the privacy of individuals. This involves organisations examining the amount and extent of personal data collected and processed, together with considering how long such information is kept and how accessible it is. Under this provision, a data subject should be protected by the strictest privacy settings while still allowing for the data subject to receive or use the product or service. Taking this approach is an essential tool in minimising privacy risks and building trust as well as being compliant with the GDPR itself. Even more, organisations need to approach all their project management and risk management methodologies and practices from the point of view of data protection by design. This will entail integrating core privacy considerations coupled with independent and robust privacy impact assessments ("**PIAs**").

PIAs are of fundamental importance under the GDPR. They are an integral part in taking a data-by-design approach and making sure that all internal processes and eventual privacy codes are also compliant with the concept of data protection by design. Besides data minimisation and pseudonymisation, other methods can be staff training programmes, audit and policy reviews an implementation of new procedures.

When implementing the principle, Article 25 of the GDPR suggests considering the following aspects:

- the state of the art (available technology);
- the cost of implementation;
- the nature, scope, context and purpose of the data processing; and
- the risks to natural persons and their severity.

As the measures to be taken are subject to the data processing activities of the relevant organisation, the review of above factors are unavoidable before implementation.

In summary, organisations should consider the data protection implications of a given processing activity at an early stage, rather than merely at the time of collection or processing. Given the provisions of the GDPR, the obligations and responsibility on organisations in the area of data protection are only set to increase.

/ Right to be forgotten

The right to erasure, also known as the right to be forgotten, is intended to enable an individual to request the removal of personal data concerning him or her from a search engine in certain specified situations set out in **Article 17 of the GDPR**. Controllers must respond without undue delay (i.e. within one month, although this time period may be prolonged in complicated cases).

The implementation of Article 17 is a response to the judicial decision of the Court of Justice of the European Union case of *Google Spain v Mario Costeja González*. Mr Gonzalez wanted to remove the data regarding his attachment and garnishment proceedings that was still available after entering his name in the search engine Google.com, although the proceedings had long since been concluded. The court found that Google was obliged to do so.

Under Article 17 of the GDPR the controller is obliged to erase personal data where one of the following grounds applies:

- The data is no longer necessary for the purpose collected or processed;
- The data subject withdraws consent and no legal grounds for processing remain;
- The data subject objects to the processing;
- The processing does not otherwise comply with the GDPR.

Anyone who feels that they will be damaged by the processing of their personal data may request the erasure of such data. However, such right is limited by the right of freedom of expression and the right of free access to information.

This means that the obligation does not apply if the processing is necessary:

- for the exercise of the right of freedom of expression and information;
- for compliance with an obligation under Union or Member State law;
- for performance of a task that is in the public interest;
- for public health reasons;
- for archiving, research or statistical purposes;
- for the establishment, exercise or defence of legal claims.

The controller itself considers the seriousness and possibility of damage with regard to such relevant factors as the extent and context of the subject's personal data. The data controller is also obliged to inform other controllers who are processing the relevant data about the subject's request of erasure of any links to those data, considering the technology available and costs of such action.

/ Co-operation and consistency between supervisory authorities under the GDPR

In the light of the globalisation and growing volumes of personal data transfers, new rules not only expand the territorial reach of the tightened data protection regime beyond the boundaries of EU territory, but also set new rules for intra-community cross-border processing of personal data. In order to ensure information exchange and to enhance collaboration for the purpose of effective investigations and proper oversight over the regulated cross-border processing, it was deemed necessary to promote closer **cooperation** between different supervisory authorities of the EU Member States. Furthermore, a **consistency mechanism** was established to foster the consistency and homogenous application of the GDPR and the powers of the national supervisory authorities were modified to realise this.

Cross-border cooperation

The GDPR contains a general rule of cooperation between supervisory authorities and introduces a new legal concept for the appointment of a leading supervisory authority "**one-stop shop**" which will lead the investigations, coordinate other concerned supervisory authorities and their operations, draft decision and submit them to the other supervisory authorities. However, the one-stop-shop mechanism can be triggered only in the context of cross-border processing.

Cross-border processing

According to Article 4 paragraph 23 of the GDPR, cross-border processing is either:

- the processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

In view of this, as soon as processing of personal data substantially affects data subjects in more than one Member State or as soon as the processing of personal data takes place in the context of the activities of respective entrepreneurial establishments in more than one Member State, the one-stop-shop mechanism will be triggered.

Competence of the supervisory authority

According to Article 56 of the GDPR, the supervisory authority of the country where the main establishment/single establishment of the company is based will be the lead authority. However, if a company carries out several different cross-border processing activities and the

decisions on the means and purposes of processing are taken in different establishments, there will be more than one lead supervisory authority. For example, if a bank has its main establishment in a certain Member State where all decisions on the purposes and means of the processing of personal data are taken except decisions concerning processing of personal data for the purposes of its insurance business, the lead authority will be determined by means of the location of the "decisive" establishment in respect to the concerned personal data.

Cases where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment will be resolved by the **European Data Protection Board** ("**Board**") depending on the complexity in one or two months from the referral of the subject-matter by a two-thirds majority of the members of the Board.

The consistency mechanism plays a key role in ensuring proper cooperation between the supervisory authorities mainly by the means of **mutual assistance** and **joint operations**. Yet unlike the one-stop-shop mechanism, the consistency mechanism has also the function of ensuring **consistent application** and **dispute resolution**, meaning that it can also be triggered in non-cross-border processing.

The Board issues opinions where a competent supervisory authority intends to adopt a measure:

- aiming to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35 paragraph 4;
- concerning a matter pursuant to Article 40 paragraph 7 whether a draft code of conduct or an amendment or extension to a code of conduct complies with the GDPR;
- aiming to approve the criteria for accreditation of a body pursuant to Article 41 paragraph 3 or a certification body pursuant to Article 43 paragraph 3;
- aiming to determine standard data protection clauses referred to in point (d) of Article 46 paragraph 2 and in Article 28 paragraph 8;
- aiming to authorise contractual clauses referred to in point (a) of Article 46 paragraph 3; or
- aiming to approve binding corporate rules within the meaning of Article 47.

In order to ensure the correct and consistent application of the GDPR in individual cases, the Board is required to adopt a binding decision which should be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

Each supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide whether it will handle the case pursuant to the provision on cooperation be-

tween the lead supervisory authority and other supervisory authorities concerned, or whether the supervisory authority which informed it should handle the case at a local level.

The one-stop-shop mechanism may prolong the investigations and lead to stricter decisions, especially in some Member States which until now did not pay proper attention to effective and proper data protection and which did not impose deterrent penalties for data protection breaches. Furthermore, it remains unclear how the one-stop-shop mechanism will work in practice and whether it will not allow for forum shopping.

/ Enforcement rules

Data subjects have the following rights against controllers and processors:

- **the right to lodge** a complaint with the supervisory authorities;
- the right to an **effective judicial remedy** where a competent supervisory authority fails to deal with a complaint;
- **the right to bring an action** against the controller or processor, whereby
  - the plaintiff should have the choice to bring the action before the courts of the state where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority;
- **the right to compensation** from the controller or processor, whereby
  - the controller or processor should compensate any damage which the data subject may suffer as a result of infringement of the GDPR; however it should be exempted from liability if it proves that it is not in any way responsible for the damage.

/ Administrative fines

The supervisory authority may impose an administrative fine of a significant amount on either the controller or the processor. The general conditions for imposing such fines are set **in Article 83 of the GDPR**. The Imposition must be effective, proportionate and dissuasive and the circumstances of each individual case should be taken into consideration.

Regard must be given especially to the following:

- the nature, gravity and duration of the infringement
- the intention or negligent character of such infringement
- the actions taken by the controller or processor to minimise the damage
- the degree of responsibility of the controller or processor, etc.

Depending on the seriousness of the infringement, the controller or processor will be subject to an administrative fine of up to **€10,000,000** or up to **2%** of its total worldwide annual turnover.

In the case of an infringement of the basic principles for processing or data subjects' rights or non-compliance with a supervisory authority order, an administrative fine of up to **€20,000,000** or up to **4%** of the total worldwide annual turnover of the preceding financial year will be imposed.

Each Member State may lay down rules on other penalties applicable for infringements not subject to fines and is required to notify the Commission of these by 25 May 2018.

/ Your Contacts

JUDr. Ing. Jaroslav Tajbr

Senior Associate, Czech Republic
T +420 233112142
jaroslav.tajbr@noerr.com

Eszter Sieber-Fazakas, LL.M.

Senior Associate, Hungary
T +36 1 2240900
eszter.fazakas@noerr.com

Mgr. Michal Bunda

Associate, Slovakia
T +421 2 59101010
michal.bunda@noerr.com

Andreea Suciu, LL.M.

Senior Associate, Romania
T +40 21 3125888
andreea.suciu@noerr.com

Arkadiusz Rumiński, LL.M.

Associated Partner, Poland
T +48 22 3788500
arkadiusz.ruminski@noerr.com

Marta Walędziak-Skowrońska

Senior Associate, Poland
T +48 22 3788503
marta.waledziak-skowronska@noerr.com

/ About Noerr

Noerr stands for excellence and entrepreneurial thinking. With well-versed teams of strong characters, Noerr devises and implements solutions for the most complex and sophisticated legal matters. United by a set of shared values, the firm's 500+ professionals are driven by one goal: the client's success. Listed groups and multinational companies, large and medium-sized family businesses as well as financial institutions and international investors all rely on the firm.

Entrepreneurial thinking

Noerr's advisors make their clients' challenges their own and are always thinking one step ahead. In doing so, they assume responsibility and are at liberty to make their own decisions. The firm is committed to always going the extra mile for its clients and to resolving complex matters with the perfect mix of experience, excellence and sound judgement.

Innovative solutions

In complex and dynamic markets new approaches are regularly required – and delivered by experts who bring both the know-how and the necessary passion. This is precisely what Noerr excels at: implementing integrated and innovative solutions in the most efficient way.

Global reach

As one of the top European law firms, Noerr is also well established internationally. With offices in eleven countries and a global network of top-ranked "best friends" law firms, Noerr is able to offer its clients truly cross-border advice. In addition, Noerr is the exclusive member firm in Germany for Lex Mundi, the world's leading network of independent law firms with in-depth experience in 100+ countries worldwide.

Capacity in Central and Eastern Europe

Noerr has long had its own offices in all major Central and Eastern European capitals. The firm regularly advises on greenfield investments, joint ventures, acquisitions and divestments in Central and Eastern Europe by investors from all over the world. With around 100 professionals, Noerr is one of the leading law firms in the region.

Noerr Group

Noerr LLP – Noerr Consulting AG – TEAM Treuhand GmbH – NOERR AG Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Offices

Alicante, Berlin, Bratislava, Brussels, Bucharest, Budapest, Dresden, Düsseldorf, Frankfurt, Hamburg, London, Moscow, Munich, New York, Prague, Warsaw

General Data Protection Regulation

Bucharest, Budapest, Bratislava, Prague & Warsaw, June 2017

/ Offices

Alicante
Noerr Alicante IP, S.L.
Avenida México 20
03008 Alicante
Spain
T +34 96 5980480

Berlin
Noerr LLP
Charlottenstraße 57
10117 Berlin
Germany
T +49 30 20942000

Bratislava
Noerr s.r.o.
AC Diplomat
Palisády 29/A
811 06 Bratislava
Slovak Republic
T +421 2 59101010

Brussels
Noerr LLP
Boulevard du Régent
1000 Brussels
Belgium
T +32 2 2745570

Bucharest
S.P.R.L. Menzer & Bachmann - Noerr
Str. General Constantin
Budişteanu nr. 28 C, Sector 1
010775 Bucharest
Romania
T +40 21 3125888

Budapest
Noerr & Partners Law Office
Fő utca 14-18
1011 Budapest
Hungary
T +36 1 2240900

Dresden
Noerr LLP
Paul-Schwarze-Straße 2
01097 Dresden
Germany
T +49 351 816600

Düsseldorf
Noerr LLP
Speditionstraße 1
40221 Düsseldorf
Germany
T +49 211 499860

Frankfurt am Main
Noerr LLP
Börsenstraße 1
60313 Frankfurt am Main
Germany
T +49 69 9714770

Hamburg
Noerr LLP
Jungfernstieg 51
20354 Hamburg
Germany
T +49 40 3003970

Kiev
Cooperation Partner:
TOV Nobles
Vul. Khreschatyk 7/11
01001 Kiev
Ukraine
T +380 44 4953080

London
Noerr LLP
Tower 42
25 Old Broad Street
London EC2N 1HQ
United Kingdom
T +44 20 75624330

Moscow
Noerr OOO
1-ya Brestskaya ul. 29
P.O.B. 247, 125047 Moscow
Russian Federation
T +7 495 7995696

Munich
Noerr LLP
Brienner Straße 28
80333 Munich
Germany
T +49 89 286280

New York
Noerr LLP
Representative Office
885 Third Avenue, Suite 2610
New York, NY 10022
USA
T +1 212 4331396

Prague
Noerr s. r. o.
Na Poříčí 1079/3a
110 00 Prague 1
Czech Republic
T +420 233112111

Warsaw
Noerr Biedecki sp.k.
ul. Grzybowska 87
00-844 Warsaw
Poland
T +48 22 3788500

noerr.com

Alicante
Berlin
Bratislava
Brussels
Bucharest
Budapest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moscow
Munich
New York
Prague
Warsaw

noerr.com