PRIVACY EUROPE

General Data Protection Regulation

Information Sheet

01.03.2016

PRIVACY EUROPE is a network of legal experts who provide advice on both the general data protection framework as well as each countries legislation. In order to give an overview of the upcoming General Data Protection Regulation, the network partners have worked together on providing information on the core aspects of the regulation, concluding with suggestions for companies on what do next, in order to be prepared.

Content:

The General Data Protection Regulation

Since 2012, ongoing efforts for creating a single set of data protection regulations have taken place. After almost four years of negotiations and debates in the end of December 2015 the European Commission, the European Council and the European Parliament agreed on the final version of a General Data Protection Regulation. After a transitional phase the regulation is to come into force in the beginning of 2018.

The regulation aims at creating a uniform data protection standard within the European Union.

The following articles are aimed at giving a rough overview of the regulation's key aspects pointing out changes to the European Data Protection Directive 95/46/EC and introducing new aspects and mechanisms.

The conclusion summarizes what companies should consider in the face of the Data Protection Regulation.

Different types of personal data including their definition

Castrén & Snellman Attorneys Ltd. | Finland
Website: www.castren.fi

Main concepts and definitions set forth in Data Protection Directive 95/46/EC will not radically change with the new regulation. However, some new subcategories of personal data, which have earlier been based on court or authority practice only, are now being codified by the regulation.

Personal data means any information relating to a data subject, who is

- an identified natural person
  - a person who can be distinguished from other members of a certain group, for example by name, or
- an identifiable natural person, i.e. a person who can be directly or indirectly identified
  - for example, based on information that makes identifying a person by reasonable means possible, such as IP address (article 4 (1)).

Special categories of personal data, often referred to as 'sensitive data'

- Special categories of personal data include personal data revealing
  - racial or ethnic origin,
  - political opinions,
  - religious or philosophical beliefs,
  - trade-union membership,
  - genetic data,
  - biometric data in order to uniquely identify a person
  - data concerning health,
  - data concerning sex life and sexual orientation, or
  - data concerning criminal convictions (article 9 and 9a).
- As a principal rule, processing of these special categories of data is prohibited. However, there are exceptions that allow processing of such data in many occasions (see Chapter 2 for Legal Grounds for Data Processing).

In addition, the regulation defines the following subcategories of personal data:

- Pseudonymous data is data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is secured and stored separately (article 4 (3b)).
- Genetic data means all personal data relating to the genetic characteristics of an individual (article 4 (10)).
- Biometric data means any personal data relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms their unique identification (article 4 (11)).
- Data concerning health means any personal data related to the physical or mental health of an individual (article 4 (12)).

Introduction of new rights of the data subject

Mónica Oliveira Costa
Coelho Ribeiro & Associados | Portugal
Website: www.cralaw.com

The Regulation enhances current data subject rights, explicitly foresees other rights and entitles the data subject with new rights.

Current data subject rights enhanced

(i) Information – It must be transparent and easily accessible and provided in an intelligible form, using clear and plain language for the target audience (particular attention must be given to children). Its content is also added with: name and contact of the DPO; legitimate interests of the controller or third party in case such legitimate interests are the processing's legitimate basis; retention period; access, rectification or erasure or restriction and object rights as well as data portability right; right to withdraw consent when the latter is the processing's legitimate basis; right to complain to the DPA; international transfers; existence of automate decision, including profiling, and meaningful information on the logic involved and consequences for the data subject; further processing for a different purpose (where applicable); and sources of data (if applicable).

(ii) Access – Electronic means must be made available to the data subject, access request shall be provided free of charge (including the first copy of the personal data) and without undue delay and no later than 30 days, which can be extended for two months when necessary (assessment based on the complexity and number of requests).

(iii) Rectification – Obtain completion of incomplete personal data, including by means of a supplementary statement.

(iv) Object – If the processing is based on public interest or legitimate interests of the controller as well as for scientific or historical purposes or statistical purposes. The data subject can also object, without the need to provide any justification, to processing for marketing purposes, including profiling.

Other data subject rights expressly foreseen

(i) Right to lodge a complaint with a DPA;

(ii) Judicial remedy against DPAs, controllers and processors;

(iii) Right to compensation and liability for any material or immaterial damages suffered and caused by the processing which is not compliant with the Regulation;

(iv) Class actions by bodies, organisations or associations on behalf of the individuals.

New data subject rights

(i) Right to be forgotten and to erasure – data subjects are entitled to have their data erased, including by third parties, without undue delay, in the following cases: the data are no longer needed for the purpose for which they were collected; the consent is withdraw; the data subject objects to the processing; comply with a legal obligation applicable to the controller; the processing is unlawful or, within information society services, offered to children under 16 years old.

(ii) Right to restriction of processing – data subjects are entitled to obtain the restriction of the processing from the controller in the following cases: the accuracy of the data is contested, the processing is unlawful, the data is no longer needed for the controller but are required for the data subject's legal claims or the data subject objects to the processing.

(iii) Right to data portability – data subjects are entitled to have copy of personal data in a structured and commonly used electronic format to allow further use thereof in case the processing is based on consent or a contract and is carried out by automated means as well as, where feasible, to obtain the transmission to another controller.

(iv) Profiling - data subjects are entitled not to be subject to a measure based on profiling, except in specific circumstances and provided that additional safeguards are in place.

Legal grounds for data processing

Desislava Krusteva
Dimitrov, Petrov & Co. | Bulgaria
Website: www.dpc.bg

Under the Data Protection Directive, in order for data processing to be legitimate, it shall satisfy at least one of the criteria set up in its Article 6. In general this legal setting will remain unchanged under the Data Protection Regulation and the requirement remains that processing shall be lawful if at least one of the legal grounds provided is satisfied.

The legal grounds for lawful data processing remain rather unchanged. Further to listing these legal grounds (which as a rule involve consent obtained from the data subject, performance of a contract, compliance with a legal obligation, protection of vital interests of the data subject, performance of a task carried out in the public interest and legitimate interests pursued by the controller), the Regulation introduces certain rules regarding the further processing of data for purposes other than the one they were initially collected.

The Regulation provides for some further clarifications regarding the meaning and the scope of some of the legal grounds for lawful data processing as the compliance with a legal obligation. It is made unambiguously clear that the controllers will be allowed to process personal data for compliance with their legal obligations only if these obligations are laid down by Union law or Member State law to which the controller is subject, which generally exclude the opportunity to process personal data for compliance with third country's law.
The Regulation also adopts a more detailed approach with regard to one of the legal grounds for the processing, namely the consent of the data subject.

The Regulation introduces a new article on the conditions relating to the consent. First of all, the burden of proof will fall on the data controller who will be obliged to demonstrate that the consent was given by the data subject to the processing of their personal data. Second, if the data subject's consent is to be given in the context of a written declaration which also involves other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Third, the Regulation provides for the rights of the data subject to withdraw the given consent at any time. The withdrawal should not affect the lawfulness of processing based on consent before the withdrawal. Forth, the Regulation provides for specific criteria for assessing whether the consent is freely given. In particular, in such cases utmost account should be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract.

It is noteworthy that the definition of the notion of data subject's consent has also been slightly modified. The definition is amplified by the newly introduced reference to the fact data subjects may provide their agreement to the processing either by a statement or by a clear affirmative action. However, the dismissal in the Regulation of the word "explicit" from the definition of consent brings up some uncertainties and leads to believe that although the consent shall be established through at least a clear affirmative action, it does not need to be explicitly demonstrated but may be implied by the data subject's actions.

The Regulation introduces a separate Article 8 specifically dealing with the consent of children. When offering services pertaining to the information society directly to a child, the processing of personal data of a child below the age of 16 years, or if provided by Member State law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that the consent is either given or authorized by the holder of parental responsibility over the child. The data controller will be required to make reasonable efforts to verify that consent is given by the holder of parental responsibility over the child, taking into consideration available technology.

Specific categories of data ('sensitive' personal data) continue to enjoy special protection under the Regulation as was the case under the Directive. Traditionally, these categories included personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life. To this list the Regulation adds genetic or biometric data. As a rule, the processing of these specific categories of data is prohibited unless justified by one of the legal grounds provided for under Article 9(2) of the Regulation. These legal grounds are very similar to the legal grounds provided by the Directive, but the Regulation introduces a few new legitimate reasons for processing sensitive data especially in the context of the medicinal products, services and devices.

It is very important to be noted that the Regulation allows the Member States to introduce specific provisions to adapt the rules of the Regulation with regard to the processing of personal data for compliance with controller's legal obligations or for completion of a task in a public interest. Also, Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data. In this respect, it could be said that the final version of the Regulation steps back from the initial concept of unified approach to the personal data protection in all Member States.

Finally, the Regulation introduces rules regarding the processing of data relating to criminal convictions and offences and such processing would be permitted to be carried out either under the control of official authority or when the processing is authorized by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects.

Compliance and Transparency

Frederic Thu
Cabinet CILEX | France
Website: www.cabinet-cilex.com

This article aims to explain the meaning of "Compliance" in the upcoming Regulation, and focuses on the subject of Transparency - a cornerstone of democracy and of control of their personal data by citizens.

Compliance as a list of obligations

The final draft of Regulation imposes strong new duties - and huge fines if companies don't comply. Section 1 of Chapter V, “General Obligations”, begins with article 22 “Responsability of the Controller”, which states in very first line that "the processing of personal data is performed in compliance with this Regulation" – meaning that every article of the Regulation must be obeyed. The same article requires the controller to "implement appropriate technical and organisational measures to ensure and be able to demonstrate" this compliance, and, where appropriate, to “implement appropriate data protection policies”: compliance starts with Policies and Documentation, as well as Key Performance Indicators.

A prior version of the text defined those "Appropriate measures" as keeping the documentation (article 28), implementing security (art. 30), performing prior Data Protection Impact Assessment (art. 33), getting prior authorisation or consultation from the Data Protection Authority (art. 34), and designating a Data Protection Officer (art. 35). However the Parliament, the Council and the EDPS feared that controllers would focus only on those topics, on a formal level, rather than really complying with the whole Regulation. As a result, the final draft of the Regulation removed this sub-list of five main measures; Compliance in now defined against the whole Regulation.

Compliance by sanctions

Another way to define Compliance is to study which non-compliances encounter the administrative fines defined by article 79 (warning – the articles will be renumbered in the final version of the Regulation). This article defines two levels of sanctions, as exposed in our previous article.

The first level of fines applies in case of non-compliance towards:

- principles of privacy by design and by default (article 23),
- definition of joint controllers (art. 24),
- rules regarding processors and relations with them (art. 26 and 27),
- records of processing activities (documentation; art. 28);
- the data security section: lack of security (art. 30), failure to notify data breaches to the supervisory authority (art. 31) or to the data subject (art. 32);
- data protection impact assessment (article 33) and prior consultation (art 34);
- the whole section about the Data protection officer: articles 35 (designation), 36 (position) and 37 (tasks).

The same level of fines applies to violations of articles 8 (child's consent), 10 (processing not requiring identification), 26 (lack of a representative for controllers not established in the Union), 29 (lack of cooperation with the supervisory authority), 39 and 39a (certification principles, body and procedures); however such risks apply only to a minority of the controllers.

The strongest penalties should be seen as defining the main compliance points. To avoid these fines, controller shall seek Compliance about articles 5 (basic principles), 6 (lawfulness), 7 (conditions of consent) and 9 (processing of special categories of data); they will respect the data subject's rights, as defined by articles 12 to 20; they will transfer of personal data to recipient in a third country or an international organisation according to articles 40 to 44; they will comply with any obligations pursuant to supplemental Member State laws adopted unter Chapter IX (provisions relating to specific data processing situations, such as national identification number, health-related purposes, genetic data, or processing in the employment context); and they will obey any order or a temporary or definite limitation on processing or the suspension of data flows by the supervisory authority pursuant to article 53 (1b), provide access to the authority (art. 53(1)), and comply with an order by the supervisory authority as referred to in article 53(1b).

Enforcement, Risks and Sanctions

Briffa | United Kingdom
Website: www.briffa.com

Overview

As a Regulation and not a Directive, GDRP will have immediate effect on all Member States after the two-year transition period without the need for domestic implementing legislation. The GDRP will (amongst other things) provide for increased penalties (administrative fines of up to €20 million or up to 4% of annual worldwide turnover, whichever is higher) to be imposed in the event of non-compliance.

Enforcement

Complaint: Any data subject may lodge a complaint with a supervisory authority. Bodies, organisations and associations may also lodge a complaint on behalf of the data subject (separate to the data subject's complaint in the case of a personal data breach).
Judicial Remedies: Judicial remedies are available to oblige a supervisory body to act on a complaint. Judicial remedies are also available against a controller or processor. Bodies, organisations or associations may represent data subjects before the courts and supervisory authorities may engage in legal proceedings.

Jurisdiction: Proceedings may be brought in the Member State where the data subject is residing or working, in the Member State where the alleged infringement has taken place or in the Member State where the defendant is established. Courts may suspend proceedings where parallel proceedings have been commenced in another Member State. Member States are obliged to ensure rapid court actions.

Risks and Sanctions

Compensation: Any person who has suffered damage has the right to receive compensation from the responsible controller or processor. Joint and several liability for the entire amount of the damage is provided for where multiple controllers or processors are involved.

Rules on Penalties: Member States must lay down rules on penalties, to sanction infringements of the GDRP, and to ensure their implementation.

Administrative Sanctions: Administrative sanctions must be effective, proportionate and dissuasive. The amount of an administrative fine will reflect (amongst other things) the nature, gravity and duration of the breach and the degree of cooperation with the supervisory authority to remedy the breach. The GDRP provides for the following administrative sanctions:

- issuing of warnings
- regular and periodic data protection audits;
- an administrative fine of up to €20 million or up to 4% of annual worldwide turnover, whichever is higher, to be imposed on anyone who intentionally or negligently (amongst other things):
  - processes personal data without sufficient legal basis for doing so; or
  - does not implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk; or
  - does not alert or notify a data protection breach to the relevant supervisory authority or data subject; or
  - does not carry out a data protection impact assessment or processes personal data without prior authorisation from or consultation with the supervisory authority; or
  - carries out or instructs an unauthorised transfer of data to a third country or an international organisation; or
  - does not comply with an order or a temporary or permanent ban on processing or the suspension of data flows by the supervisory authority.

The "one-stop-shop" principle

Gorrissen Federspiel | Denmark
Website: www.gorrissenfederspiel.com

The new General Data Protection Regulation introduces a one-stop-shop-principle. This principle will apply only in cross-border cases where the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as the lead supervisory authority.

In this context, cross-border processing of personal data means either

(i) cases where the processing takes place in the context of activities of establishments in more than one member state and where the controller or processor is established in more than one member state, or

(ii) cases where processing takes place in the context of activities of a single establishment, but which substantially affects or is likely to substantially affect data subjects in more than one member state.

The one-stop-shop mechanism will give the data protection authority in the member state where the data controller has its main establishment (normally the place of its central administration), the opportunity to make a single supervisory decision.

The decision must, however, be based on a cooperation procedure with the data authorities in the other member states concerned and this cooperation procedure is set out in more detail in Chapter VII of the Regulation. The one-stop-shop principle is therefore predicted to provide for cooperation and joint-decision making between the European data protection authorities. The jointly agreed decision will be adopted by the data protection authority best placed to deliver the most effective protection from the perspective of the data subject.

Some of the main purposes of the one-stop-shop principle are to reduce costs and increase legal certainty. When the new rules enter into effect, companies will only have to deal with one authority instead of 28, which will make it simpler and cheaper for companies to do business in the European Union. For citizens, the rules will make it easier and more efficient to get their personal data protected. Other goals for the one-stop-shop-principle are that the single supervisory decision should be made fast, ensure consistent application, provide legal certainty and reduce the administrative burdens.

Data processing by a service provider (data processor)

AK SCHOVANEK | Czech Republic
Website: www.akschovanek.cz

1.) Unlike the Directive 95/46/EC, the General Data Protection Regulation ("GDPR") will impose some obligations and possible sanctions directly on data processors (service providers).

Main direct obligations of the data processors under GDPR include the following:

a. Maintain records of processing activities (with exceptions)
b. Co-operate with a supervisory authority
c. Implement required security measures
d. Designate a data protection officer (in specified cases)
e. Comply with the rules for international data transfers

Some of the GDPR provisions propose administrative fines of up to 10.000.000 EUR or 2% of the total worldwide annual turnover, whichever is higher, and up to 20.000.000 EUR or 4% of the total worldwide annual turnover, whichever is higher, for non-compliance, respectively. These limits shall apply for data controllers, as well as data processors.

Data controllers shall use only processors providing sufficient guarantees that the processing will meet the requirements of the GDPR. Codes of conduct and certifications for the data controllers and processors are foreseen.

2.) Data processing agreements between data controllers and processors will have to be more detailed as the GDPR is significantly more prescriptive than the Directive 95/46/EC.

According to the draft of GDPR, data processing agreements shall include following obligations of data processor:

a. Process the personal data only on documented instructions from the controller
b. Ensure that persons authorised to process personal data are under obligation of confidentiality
c. Implement security measures required by GDPR
d. Enlist sub-processor only with prior written consent of the data controller
e. Assist controller with measures for the fulfillment of data subjects' rights
f. Assist controller in ensuring compliance with security requirements and breach notification, data protection impact assessment and prior consultation obligations of the GDPR
g. At the choice of controller, delete or return all personal data and its copies to the controller after the end of the data processing
h. Make available to the controller all information necessary to demonstrate compliance with obligations of GDPR and allow audits conducted by controller or auditor appointed by the controller

Standard contractual clauses are foreseen. Existing data processing agreements will probably have to be renegotiated and the agreements being negotiated now should be future proofed if possible.

3.) According to the draft of GDPR, data processors shall be liable for the damage caused by the processing where they have not complied with obligations of the GDPR specifically directed to processors or acted outside or contrary to the lawful instructions of the controller.

4.) According to the draft GDPR, if data processor in breach of the GDPR determines the purposes and means of data processing, it shall be considered to be a controller with all respective obligations in relation to that processing.

International data transfers

Shobha Fitzke
intersoft consulting services AG | Germany
Website: www.intersoft-consulting.de

Under the European Data Protection Directive international data transfers outside the EU/EEA are restricted by the Data Protection Directive and are only permitted if the general requirements for data transfer as well as an adequate level of data protection is ensured, or one of the derogations apply.

Methods of ensuring an adequate level of data protection include EU Standard Contractual Clauses, consent by the data subject or other transfer mechanisms such as Binding Corporate Rules.

Furthermore the transfer of personal data is allowed if the commission has established that a third country ensures an adequate level of data protection.

New Aspects regarding data transfers
The previous approach will continue under the Regulation. Current adequacy decisions remain in force until amended, replaced or repealed.

However, new aspects are introduced as well:

- Binding Corporate Rules are now specifically mentioned as a valid mechanism for international data transfers. The Draft gives a detailed description of the conditions for data transfers via Binding Corporate Rules. The process is based on the current practices and requirements of supervisory authorities and is expected to facilitate the approval process.
- While the Data Protection Directive only allows for a country to be evaluated as ensuring an adequate level of data protection the Regulation stipulates that an adequate level of data protection can also exist for a territory or a sector within a country. Thus, a transfer of personal data may take place, where the Commission has decided that a country, a territory or one or more specified sectors within a third country ensure an adequate level of data protection.
- Codes of conduct (Art. 38) and certification mechanisms (Art. 39) are being introduced. If approved accordingly, data transfer is permitted.
- The derogations set out under the Data Protection Directive will continue to be valid. Additionally, data transfer which is not covered by the derogations may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller and are not overridden by the interests or rights and freedoms of the data subject.

The Data Protection Directive has been implemented differently by the EU Member States. Some Member States have adopted additional safeguards such as prior notification or authorization of the competent DPA. With the Regulation these mechanisms will no longer be required. This should largely contribute to facilitating data transfers abroad.

The role of the data protection officer (DPO)

Flavio Monfrini
ITALY LEGAL FOCUS | Italy
Website: www.ItalyLegalFocus.com

The role and responsibilities of the data protection officer ("DPO") have been two of the most discussed aspects of the General Data protection Regulation.

History of the DPO in the legislation

In the history of the negotiations of the new regulation, the Commission adopted the strictest position, by mandating the appointment of a data protection officer whenever the processing of personal data is carried out by a public authority or body, by an enterprise employing 250 persons or when core activities of the enterprise require regular and systematic monitoring of data subjects.

The European Parliament adopted a softer position, by increasing the threshold for the mandatory appointment of a DPO when the processing relates to more than 5000 data subjects in any consecutive 12-month period.

Lastly, the Council took an even more lenient approach and proposed that the appointment of a DPO must be entirely voluntary, unless specifically mandated by EU or member states' law.

In Article 35 Sec. 1 of the final draft, the member states agreed that the controller and the processor must designate a DPO when:

(i) The processing is carried out by a public authority;

(ii) The core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or

(iii) The core activities of the controller or the processor consist of processing of special categories of data on a large scale.

In all other cases, the controller or processor may or, where required by Union or Member State law shall, designate a data protection officer.

Appointment

The DPO will be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the task set forth in the proposed new regulation.

The DPO may be an employee of the data controller or an external contractor, performing his/her duties on the basis of a service contract. A group of undertakings may appoint a single DPO. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority.

As the DPO may be an employee of the controller, the regulation provides that he/she cannot be dismissed, unless he/she no longer fulfills the conditions required for the performance of the DPO tasks or a dismissal is otherwise justified under local labor law. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

Role of the DPO

The DPO must be involved properly and timely in all issues relating to the protection of personal data. The DPO must be independent with regard to the performance of his/her tasks and the data controller must ensure that other tasks or duties entrusted with the DPO do not result in a conflict of interests.

Furthermore, the regulation provides that sufficient resources must be provided to the DPO, that the DPO must not be penalized for performing his/her tasks and that the DPO must report directly to the highest management level of the controller.
Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.

Tasks of the DPO

Among the tasks of the DPO, the proposed regulation (as amended by the Council, which deleted several of the tasks proposed by the Commission) sets forth the following:

- Inform and advice in connection with the processing of personal data;
- Monitor compliance with the regulation and local data protection legislation;
- Advice in connection with the data protection impact assessment;
- Liaise with data protection authorities and act as their contact point.

- Have due regard to the risk associated with the processing operations

Conclusions

Article 35 Sec 1 establishes the obligation to appoint a DPO when certain categories of processing operations, specifically listed, are carried out. On the other hand, Sec. 4 of Article 35 provides that in all other cases the appointment is not mandatory, if not required by Union or Member State law. This means that the Council's initial proposal of a mandatory appointment of the DPO did not prevail. However, it also means that significant differences among member states may emerge in relation to the mandatory appointment of a DPO, thus defeating the main purpose of the new regulation, which is to create a single legal framework for all EU countries.

Profiling

Olivier Oosterbaan
Leopold Meijnen Oosterbaan | The Netherlands
Website: www.leopoldmeijnenoosterbaan.nl

Profiling, in good and bad forms, has taken an enormous flight in recent years with the availability of huge amounts of data that is more and more interconnected. Enough reason for the European institutions to adopt new limitations on profiling and automated decision making based on the resulting profiles in the new EU General Data Protection Regulation (GDPR).

Profiling

Profiling covers the use of personal data "to evaluate personal aspects relating to a natural person", and to use that data in turn for prediction or analysis of that person's performance at work, economic situation, location (which would include movement), health, personal preferences (and interests), reliability or behavior.

While this may have been written against the background of obviously negative (biased) profiling resulting in significant consequences for the data subject, such as in the fields of labor, banking and insurance, it will also cover many cases of (arguably) less damaging fields like social media and online marketing, and many data controllers will have to assume their processing falls under it.

Automated decision making

Where profiles are used for automated decision making, the GDPR includes a right for the data subject not to be subject to such automated individual decision making with legal effects or significant consequences unless necessary for:

- performing a contract with the data subject,
- based in law, or
- with explicit permission from the data subject.

Significantly, the new Regulation introduces an obligatory element of human review: each data controller that uses profiling to perform a contract or with permission from the data subject needs to include the possibility of "human intervention" to review any automated decision after it is made. This will require a significant effort from the data controller in the design and operations of its data processing systems, including the training of staff to conduct such reviews.

Big Data

PD Dr. Simon Schlauri
Ronzani Schlauri Attorneys | Switzerland
Website: www.ronzani-schlauri.com

Until a few years ago, only data from relatively rigidly designed databases could be processed. For instance, one could query the telephone number based on the name or the birthday of a person. Today, newer "big data" technology allows for the processing of an unlimited number of variably structured data in real time. Relations between different data from countless sources, which were originally collected for completely different purposes, can be established. The term "big data" or "big data analysis" therefore refers to the processing of large, complex, and rapidly changing data sets.

Some typical applications for big data analysis are:

- Precise personal alignment of online advertising and cross-selling;
- Market research;
- Detection of irregularities in financial transactions;
- Prediction of epidemics;
- Intelligence work.

Big data analysis does not necessarily focus on personal data (with reference to individuals). As long as anonymous data is processed, big data will not raise data protection issues (e.g., if only weather data is processed). However, as big-data analysis may allow for a de-anonymization of originally anonymous data, the distinction between (non-regulated) anonymous data and personal data becomes blurred.

In cases where personal data is processed, big data analysis may raise a number of data protection issues:
for instance, without the express and informed consent of the user the processing of sensitive data, such as, health, racial origin, trade-union memberships or sexual orientation, are often prohibited. This principle of informed consent may be violated by big data analysis if various data sources are linked because the purpose of the data processing cannot be foreseen at the time of collection; therefore, informed consent cannot be given beforehand. For the same reason the principle of transparency on data processing can hardly be safeguarded. In many cases, the principle of data minimization is violated because more data is collected for exploitation by big data analysis than necessary for the provision of the service for which the data is originally collected.

The new EU General Data Protection Regulation (GDPR) will render European data protection rules more stringent, in particular in the context of big data analysis. The regulation aims at increasing the transparency and consent principles and at introducing requirements for privacy by design and privacy impact assessments.

In particular, if the processing is based on the data subject's consent, the request for consent must be presented in a distinguishable way from the other matters and in clear and plain language. Consent may be withdrawn at any time. It must be freely given, which means that the performance of a contract, including the provision of a service, may not be made conditional on the consent to the processing of data that is not necessary for the performance of this contract.

Another new provision deals with further processing in comparison to the original purpose declared to the data subject. It defines the factors to be considered in determining whether an additional purpose is compatible with the original purpose, and the possibility for processing data for incompatible purposes in certain limited circumstances. Where the purpose of further processing is incompatible with the original purpose such further processing must have a legal basis pursuant to the GDPR.

In particular, such a legal basis is given in the case of legitimate interests pursued by the data controller or by a third party. Such legitimate interest could exist, for example, if there is a relevant and appropriate connection between the data subject and the data controller: e.g., the data subject is a client or supplier of the controller. The assumption of a legitimate interest will require careful assessment (a "balance test"), including whether a data subject can expect at the time and in the context of the collection of the data that further processing may occur. In particular, such assessment must take into account whether the data subject is a child, given that children deserve specific protection.

Whereas the new General Data Protection Regulation is clearly tightened in certain aspects, it remains difficult to assess how this balance test will be applied by the courts: While it seems to offer a lot of scope to the industry, its field of application might be reduced by fundamental rights considerations.

Data protection in the Cloud

Victor Salgado
Pintos & Salgado Abogados | Spain
Website: www.pintos-salgado.com

Today it is very common to use cloud computing services and technologies which implies that a large amount of personal data are being transferred internationally to third countries with important obligations and responsibilities from the new EU Regulation. These are the main ones:

Information to the data subject

Above all, the Regulation refers a needed information that must be given to the data subject by the controller, where applicable, that it intends to transfer data to a third country or international organisation, which is probable when cloud computing is used to store or process the personal data.

Here both previous versions of the Regulation differ from the last one from the Council. Meanwhile, this does not refer any more information except that a right of access is executed, the Commission's version add the level of protection afforded by that third country by reference to an adequacy decision by the Commission and, the European Parliament's version also includes a reference to the appropriate safeguards and the means to obtain a copy of them.

In this sense, the last document with the analysis of the final compromise text with a view to agreement, adopted in Brussels on December 15th of 2015, confirm the referred draft from the European Parliament only adding the indication of where the appropriate safeguards information has been made available in alternative to the indication of the means to obtain a copy of them.

Documentation

Regarding the use of cloud computing services, each controller and processor shall, where applicable, maintain a list of the intended transfers of data to a third country, including the identification of them and, in such case, the documentation of appropriate safeguards under the Regulation.

Prior authorisation and prior consultation

To ensure compliance with the Regulation and to mitigate the risks involved in the eventual cloud processing, the controller or the processor shall obtain an authorisation from the supervisory authority prior to such processing of personal data, where a controller or processor adopts specific contractual clauses or does not provide for the appropriate safeguards in a legally binding instrument for the transfer of personal data to a third country.

Transfers with an adequacy decision

If the cloud processing implies an international transfer, as it often does, it may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. In such case, that transfer shall not require any specific authorisation.

Transfers by way of appropriate safeguards

If the destination country of the cloud processing does not ensure an adequate level of protection, the controller or processor must adduce appropriate safeguards with respect to the protection of personal data by means of a legally binding instrument under the Regulation.

Also, prior authorisations by a supervisory authority on the basis of Article 26.2 of Directive 95/46/EC shall remain valid until two years after the entry into force of the new Regulation unless amended, replaced or repealed by that supervisory authority before the end of this period.

Special reference to the "Safe Harbor":

As most of cloud computing services providers are located in the US, as Amazon, Google, Microsoft and so on, it is important to refer to the recent Judgment from the Court of Justice of the European Union of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, which declared that the Commission's US Safe Harbor Decision of 26 July 2000 is invalid. This urges any controller or processor that processes personal data in the cloud, with a US provider, to seek another legal basis for an adequate Regulation implementation.

Data protection in the Workplace

Elena Spiropoulou
Spiropoulou Law Firm | Greece
Website: www.cyberlaw.gr

The Regulation directly affects the data subjects' rights in the workplace, as new definitions and obligations for the employers are set.

Definitions

(i) Consent of data subject (employee) to the processing of his/her data must be 'explicit'. This criterion is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent. This applies especially in case where the data subject is in a situation of dependency from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context.

(ii) A definition of "enterprise" is set: Enterprise means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(iii) "Group of undertakings" means a controlling undertaking and its controlled undertakings;

(iv) Enterprises where the core activities of the controller or processor consist of processing operations, which require regular and systematic monitoring a mandatory, a "data protection officer" has to be appointed by the employer. This obligation also exists where the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9.

Employer's rights

Processing of sensitive personal data is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards.

Data subject's rights

(i) Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes.

(ii) An employee has the right not to be evaluated and not to be subject to a measure based on profiling.

Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of recruitment, performance of the employment contract, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Conclusion

As you can see from the different topics, the implementation of the General Data Protection Regulation will change some main data protection issues. European as well as international companies should be aware of these changes and should prepare themselves for these changes soon in order to be compliant with the upcoming regulation.

But what can be done now to be prepared?

The following questions and issues should give you an idea on what you should focus on in the next few months.

- Think about strategies for implementation of a data privacy concept and appointment of a data protection official. Review your data protection policies and privacy policies. What are the processes? When is the DPO involved?
- Businesses processing personal data of minors under 13 on the basis of consents will need to prepare strategies for obtaining guardian consents or authorisations
- If your company uses profiling methods (i.e. for marketing purposes): Review current information notices and your privacy policy to ensure that they are accurate, comprehensive, and up to date. Be sure to use correct opt-in/consent procedures if applicable ("datamining")
- Work-flows for data subject rights should be in place (deletion, erasure, access)
- Do you outsource a lot of tasks to data processors (which process personal data on your behalf)? How is this handled? Is a data processor agreement in place? Does the processor use appropriate security standards? Has a risk assessment taken place? Is it secure to outsource these tasks?
- If you act as a processor: are you officially certified regarding your security standards? Are contracts in place which meet the standards?
- Do you transfer data abroad? In and outside Europe/EEA? Is your company incorporated in a worldwide corporate structure? On what legal basis do data transfers happen? BCRs? EU model clauses?
- What about sub-contractors? Think about intercompany agreements!
- Do you have risk assessment measures in place for data processings? Think about the one-stop-shop principle, work with DPA for registration/notification. Is someone in your company responsible for communication with the DPA?
- Work within your corporate structure for data privacy compliance, don't only rely on your national laws!
- Review your contracts with third parties on data protection issues (liability clauses)
- Train your staff in data privacy
- Keep in mind that specific employee data protection rules may be passed by individual member states, which would prevent a high degree of harmonisation in this area.
- Create a "data privacy team" with members from different jurisdictions in your corporate group which should be trained in data privacy matters.
- Think globally!