aura portal

GDPR

General Data Protection Regulation (GDPR) is a European Union regulation on the protection of natural persons with regard to the processing of personal data which will be enforceable from 25 May 2018.

INDEX

What is GDPR and who does it affect?

On April 27 2016, the European Parliament and the Council ratified the Regulation (EU) 2016/679. The purpose of this regulation is to protect all European citizens' personal data and will come into force on May 25, 2018. This regulation applies to "the total management or partially automated processing of personal data and non-automated personal data contained or intended to be included in a file ".

As regards the territorial scope, as set out in Article 3, the regulation applies "to the processing of personal data in the context of the activities of a controller (organization that collects data from EU residents) or a processor (organization that processes data on behalf of data controller e.g. cloud service providers) in the Union, regardless of whether the processing takes place in the Union or not. ". In the case of goods or services and the control of user behavior, this regulation will apply whenever the personal data is from an E.U. resident, regardless of the place of establishment of the person responsible for such data.

So, in summary, GDPR applies to any company, inside or outside the E.U., that offers goods and services to European citizens.

What are the obligations under the GDPR?

The law states that the use of data must be lawful, fair and transparent for the data subject (person) and must be collected for explicit and legitimate purposes, not allowing further treatment in a manner incompatible with those principles. The data should be relevant and limited to the information necessary for the purposes for which they are treated. It should also allow the rectification and deletion of inaccurate data.

The data must be maintained in such a way that it is not possible to identify the parties after it has been processed for its initial purpose and must have guaranteed security to avoid unauthorized or unlawful processing, loss, destruction or accidental damage.

Ensure the lawful and transparent use of data

For processing to be lawful, at least one of these conditions must be met:

A. The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

B. Processing is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract.

C. Processing is necessary for compliance with a legal obligation to which the controller is subject.

D. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

E. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

F. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Some of the above points are applicable to public administrations. Most companies will meet criteria A, i.e., they will have the subject's consent and be able to demonstrate this consent.

Recommendation: review the contracts currently in force with providers and customers, and if need be, modify the contracts to include "informed consent".

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall 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.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal and it should be as easy to withdraw as to give consent.

It is prohibited to process personal data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data intended to identify the form of a natural person, data relating to health or data relating to the sexual life or sexual orientation of an individual, although the regulation stipulates certain circumstances in which this prohibition will not apply.

To ensure transparent treatment, where personal data relating to a data subject are collected, the controller shall, at the time when personal data are obtained, provide the data subject with the following information:

- The identity and the contact details of the controller and, where applicable, of the controller's representative.

- The contact details of the data protection officer, where applicable.

- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

- The legitimate interests pursued by the controller or by a third party.

- The recipients or categories of recipients of the personal data, if any.

- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission.

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

- Where data subject has given consent to the processing of his or her personal data for one or more specific purposes, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- The right to lodge a complaint with a supervisory authority.

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

- The existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the

data subject.

In addition to the information referred to above, where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- The categories of personal data concerned.

- Any available information as to their source.

The data subject's right to access, rectify and erase personal data

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- The purposes of the processing.

- The categories of personal data concerned.

- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations.

- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

- The right to lodge a complaint with a supervisory authority.

- Where the personal data are not collected from the data subject, any available information as to their source.

- The existence of automated decision-making, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

- The data subject withdraws consent.

- The data subject objects to the processing on grounds relating to his or her particular situation and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes.

- The personal data have been unlawfully processed.

The data subject shall have the right to restrict processing if they contest the accuracy of the personal data, for a period enabling the controller to verify its accuracy;

if the processing is unlawful and the data subject opposes its erasure and requests the restriction of their use instead; the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.

Where processing has been restricted as described above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

The data subject shall have the right to transmit personal data to another controller without hindrance from the controller to which the personal data have been provided, shall not adversely affect the rights and freedoms of others

Data Controllers, Processors and Data Protection Officers (DPO)

The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Where proportionate in relation to processing activities, these measures shall include the implementation of appropriate data protection policies by the controller. Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the obligations of the controller.

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

A. Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing,

unless that law prohibits such information on important grounds of public interest.

B. Ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

C. Takes all measures required for security of processing.

D. Respects the conditions for engaging another processor. The controller may oppose or authorize the appeal in writing. The same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed.

E. Assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.

F. Assists the controller in ensuring compliance with the obligations.

G. At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

H. Makes available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

For organizations of 250+ employees and smaller organization where the processing is likely to result in a risk to the rights and freedoms of data subjects, each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility in writing, including in electronic form.

The record shall be made available to the supervisory authority on request and shall contain all of the following information:

- The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.

- The purposes of the processing.

- A description of the categories of data subjects and of the categories of personal data.

- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations.

- Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization.

- Where possible, the envisaged time limits for erasure of the different categories of data.

- Where possible, a general description of the technical and organizational security measures.

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- The name and contact details of the processor or processors and of each

controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer.

- The categories of processing carried out on behalf of each controller.

- Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization.

- Where possible, a general description of the technical and organizational security measures.

The controller and the processor shall, where applicable, designate a data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the necessary tasks.

The data protection officer must be involved, properly and in a timely manner, in all issues which relate to the protection of personal data and be supported by the controller and processor. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of his/her tasks.

The data protection officer may fulfil other tasks and duties and shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks and shall report directly to the highest management level of the controller or the processor.

The data protection officer shall have at least the following tasks:

A. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions.

B. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

C. To provide advice where requested as regards the data protection impact assessment and monitor its performance.

D. To cooperate with the supervisory authority.

E. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter.

Security of processing

The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymisation and encryption of personal data.

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

• A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification shall at least:

A. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

B. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.

C. Describe the likely consequences of the personal data breach.

D. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall not be required if any of the following conditions are met:

A. The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

B. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

C. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Conclusion

This new data protection regulation establishes a greater control of data processing and enforces its protection. In the event of a security breach, the competent

authority must be notified within 72 hours. In addition, a new role has been established, which is the Data Protection Officer (DPO), whose responsibility is to ensure GDPR compliance.

AuraPortal can help you to comply with GDPR by automating your processes and establishing control filters on the data processed. It uses a "Data Protection Center" to centralize the accessibility and management of all processes related to the GDPR regulation.

Definitions

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Filing System means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to

the purposes of the processing.

Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Consent consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Genetic Data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric Data means personal data resulting from specific technical processing relating to the physical, physio logical or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Data Concerning Health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Group of Undertakings means a controlling undertaking and its controlled undertakings.

Binding Corporate Rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Supervisory Authority means an independent public authority which is established by a Member State.

Supervisory Authority Concerned means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of the Member State of that supervisory authority; data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or a complaint has been lodged with that supervisory authority.

Relevant and Reasoned Objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

Information Society Service means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1).

International Organization means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.