apdcat
Autoritat Catalana de Protecció de Dades

Data protection Guidelines for schools

2018

Guide collection. Num. 3

Generalitat de Catalunya

Index

Regulation (EU) 2016/679 of the European Parliament and of the Council, 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) (hereinafter the GDPR) was passed on 27 April 2016, and has been fully applicable since 25 May 2018. This new Regulation, which is being enacted at a European level for the first time, will entail significant changes in the protection of personal data, from both the point of view of the rightsof individuals and the obligations of people and institutions that process personal data.

1. Objective

Schools play an essential role in guaranteeing the right to protection of personal data, not only as entities responsible for the proper processing of the information of the people relating to them, but also as an essential factor in its dissemination, since this can enable people – minors – to become aware of it and use it as soon as they are educated at school.

This document aims to provide the necessary support to schools in order to establish the necessary data processing policies and procedures that must be implemented as part of a school's normal routine. However, it is above all an opportunity for schools to review their practices in the sphere of data protection and privacy.

2. Schools and the GDPR: an opportunity to review compliance

2.1 Accountability the principle of proactive responsibility

The data controller, the school – in public sector schools, the Ministry of Education must establish whether the data controller is each school or the Ministry itself – must guarantee and be able to demonstrate that the processing complies with the data protection regulations and that it has adopted the most appropriate measures to guarantee the rights and freedoms of the persons whose data is processed.

This new principle requires the school to examine the data it processes, its purpose for doing so, and what type of processing it carries out. Based on this detailed knowledge, the risk involved in this processing must be assessed and the appropriate measures taken according to that assessment. One of the cases that needs to be considered beforehand due to the risks that it may entail is the processing of data from vulnerable groups, such as schools, minors, and minors with special educational needs or with disabilities.

It must be possible to demonstrate compliance before the data subjects and before the Data Protection Authority.

The school must have a conscientious, diligent and proactive attitude to all its processing of personal data.

2.2 The focus on risk

Another new feature of the new Regulation is that the GDPR adopts a focus on risk, and that the specific measures to be applied must take into account the nature, scope, context and purposes of the processing, as well as the risk to individuals' rights and freedoms. In other

words, each data controller, depending on their characteristics, will take the necessary measures with respect to the risks that exist.

According to this approach, some of the measures that the GDPR establishes should only be applied when there is a high risk to rights and freedoms, while others must be modified depending on the level and types of risk involved in the processing.

Most of the data processed in schools is data related to minors. This means that given this group's vulnerability and the possible consequences of an incorrect processing of its information, both in the present and in the future, schools must exercise extreme diligence in their processing of this information, to an even greater extent than other sectors.

These two factors (accountability and the focus on risk) influence all the obligations of organisations.

2.3 Data protection by design and by default

The Regulation introduces the concepts of privacy by design and privacy by default. This implies that the controller must apply, both when determining the means of processing and during the processing itself, the appropriate technical and organisational measures designed to effectively implement the principles of data protection (such as pseudonymisation), and integrate the necessary safeguards into the processing to meet the requirements of the Regulation.

The controller must also apply the appropriate technical and organisational measures to ensure that by default, only the personal data necessary for each specific purpose of the processing are processed.

Example

When designing an application for use in schools, the first factor to be assessed is how it affects the privacy of the students, and it must be designed with the highest level of protection. In other words, in terms of design and default, a high level of protection of students' privacy must be guaranteed.

3. Data Processing in schools

3.1 Personal data

Personal data: 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.

In order to comply with the obligations established by the data protection regulations, the data that is to be processed and that must be protected must be identified, and the basic concepts, fundamental principles and obligations established to guarantee the protection of the information of the data subjects or those affected must also be known.

In the case of student data, data processing in schools takes place for the first time when the parents or guardians request the place at the school during the preenrolment process, and it continues at least until the student finishes his/her studies at that school. This means that a great deal of information is processed, either provided by the family, by the professionals who work at the school (teachers, tutors, psychologists, etc.) and by the students themselves.

In order to carry out their tasks, schools process data from various groups and of different types. They should first consider whether the purpose thereof can be achieved without needing to collect data that identifies individuals, either directly or indirectly.

In order to produce the data processing "map", it is necessary to establish the following:

3.1.1 Source of the data

- The data that the school receives, e.g. when the Ministry sends the school the list of admissions.
- The data generated by the school itself, such as grades, educational psychology reports on the students, etc.
- The data that the school sends, e.g. to the school's service providers.
- The data that is send to the new school when a student changes school, etc.

3.1.2 Operations or procedures in which data are processed

- Registration and admission of students: advertising and contact with people interested in joining the school, the pre-enrolment and enrolment process.
- Academic management.

- Special educational needs.
- Services provided by the school to students apart from its educational purpose: school meals, school transport, extracurricular activities, excursions and camps, uniforms, etc.
- Management of teaching, administrative and services staff.
- Management of suppliers.
- Payment systems.
- Online teaching platforms.
- Communication/contact systems.
- Medical information.
- Services for alumni.
- Other.

3.1.3 Whose data are processed?

The data subject: any information about an identified or identifiable natural person.

- Students.
- Students' parents.
- Teachers.
- Tutors.
- Workers at the school.
- Suppliers.
- Assistants in activities.
- Monitors.
- Alumni.
- Other people with whom the school has a relationship.

The personal data that schools process when carrying out their activities do not belong to the school but instead to the students, their relatives, their personnel and the other physical persons with which they have relationships. They are the real tittle holders.

3.1.4 What data are processed?

All data that enable a person to be identified.

Some data are only useful for identifying people; others can show aspects of their personality enable evaluation of the individual or shed light on aspects of their history and circumstances (studies, family, work life, health, etc.).

- Identifying data, such as the name, address, photograph or national identity document number.

- Personal data, such as the birthplace, nationality or gender.
- Data on social circumstances, such as hobbies, lifestyle and family situation.
- Academic and professional data, such as the academic record and professional experience.
- Financial data, bank and insurance details, grants, credit cards.
- Employment history data, such as the institution, level, workplace, work history.
- Data relating to criminal offences and crimes.
- Special categories of data: data on health, ideology, trade union membership, religion, beliefs, sex life, and racial origin.

3.1.5 Special ('sensitive') categories of personal data

The GDPR classifies as special categories of data those that reveal:

- Ethnic or racial origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Processing of genetic data.
- The person's sex life or sexual orientation.
- Genetic data.
- Biometric data used for the purpose of uniquely identifying a natural person.

The GDPR has included these latter two types of data in the special categories of personal data:

Genetic data: 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: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Examples of special categories of personal data

Schools usually process data relating to special educational needs and students' health data, such as:

- Physical handicaps, such as disabilities.
- Allergies and intolerances, to organise the school meals service.
- Educational psychology, to produce reports on the students.
- Injuries or illnesses that may occur at school.
- Learning difficulties, high ability levels, ADHD, autism, etc.

This type of information must be processed particularly carefully in compliance with the principles of data protection and is subject to special conditions, both in terms of how to obtain consent and the applicable security measures.

The necessary protocols for the proper processing of this information must therefore be established, both during the school's normal routine (classroom time, recreation, physical education, school meals, nursing, psycho-pedagogical assessment, etc.) and in extraordinary situations (substitutions of teachers or tutors, celebrations of birthdays, school trips, summer camps, etc.).

The GDPR prohibits the processing of this type of data apart from specific exceptions that are listed in section IV of the document, entitled "Legitimate interests".

3.2 Who processes personal data?

3.2.1 The data controller

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 (...).

Some schools in the public sector are accountable to a Ministry of the Government of Catalonia, but at the same time they have a certain degree of autonomy in their management. The Ministry of Education will therefore determine who is the data controller.

The data controller at state-assisted schools will be the school itself.

3.2.2 The data processor

A natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller.

As data controllers, schools may commission third parties or institutions to process personal data or to undertake an activity that involves the processing of personal data, such as the organisation of:

- Extracurricular activities.
- The bus service.
- The school meals service.
- Other external services (swimming, extracurricular activities, accounting and employment advice, destruction of paper, etc.).

In this case, the data processor must be taken into consideration.

The regulation of the relationship between the data controller and the processor must be established through a contract or agreement, or a binding legal document. The contract or the legal document must be recorded in writing, including in electronic form.

The contract must at least establish the object, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. The contract must also stipulate whether the data will be returned to the controller or will be destroyed after the services have been completed.

The data controller must select a data processor who provides sufficient safeguards regarding the implementation and maintenance of appropriate technical and organisational measures, in accordance with the provisions of the GDPR, and who ensures the protection of the rights of the data subjects. A duty of diligence is therefore involved when selecting the data processor.

Links

You will find the necessary information and guidance models for the contract/ agreement for the data processor here: The data processor

What happens with the contracts arranged before the entry into force of the GDPR?

Contracts arranged before the entry into force of the GDPR in May 2018 must be adapted to respect the content thereof. Although many of the obligations that the framework established in the GDPR are already included in the Spanish regulations, existing contracts must be amended so that the clauses include all the contents of the Regulation, taking into account that the generic referrals in the article of the GDPR that regulates them are not valid.

According to the Second Transitory Provision of Royal Decree-Law 5/2018 of 27 July, on urgent measures for the adaptation of Spanish law to the European Union regulations on data protection, processing contracts and agreements established before 25 May 2018 remain in force until their expiration date.

Contracts with an indefinite duration are valid for four years from 25 May 2018 (until 25 May 2022).

In any case, during the validity of the contract or agreement, either party may request the other party to amend the contract to bring it into line with the stipulations of article 28 of the GDPR.

3.3 Record of processing activity (RPA)

Processing: 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As of 25 May 2018, the GDPR has abolished the requirement need to formally create files and notify the data protection registry of the supervisory authorities concerning these files.

3.3.1 Record of processing activity (RPA)

The data controller and processor must establish a record of the processing activities under its responsibility.

The GDPR stipulates certain exceptions to the obligation to create this record, which do not include the data processing carried out by schools.

This is a basic instrument not only for possible supervision by the Authority, but also to provide an up-to-date image of the processing taking place in the school, which is essential for risk management. The record must be in writing, including in electronic form, and must be presented to the Authority on request.

3.3.2 How is the record of processing activity organised?

The record can be organised based on specific processing activities, which are all associated with a joint basic purpose (e.g. “academic management” or “human resources and payroll management”), or according to other criteria.

Links

The APDCAT has developed a simple application to record processing activities in order to assist data controllers with their organisation. You can download it at this link: Record of processing activity application

4. Legitimate interests: when can personal data be processes?

4.1 Principles how to comply with the GDPR

Data processing must always comply with the principles established by the GDPR. One of the principles, an important new item in this regulation, the accountability principle has already been outlined above.

4.1.1 Lawfulness, fairness and transparency

Data must be processed with lawfulness, fairness and transparency.

For example, the school must provide the data subjects with information about the processing with sufficient advance notice in accordance with the established deadlines, and when changes are made to the data processing, they must be notified to the data subjects, who must receive an explanation of how these changes will affect them.

4.1.2 Purpose limitation

Data must be collected for specified, explicit and legitimate purposes and not subsequently processed in a manner incompatible with those purposes. The subsequent processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

The Organic Education Law 2/2006 of 3 May (OEL) states that the information collected by schools when performing their educational role must be strictly necessary for their teaching and guidance tasks, and it may not be processed for purposes other than education without specific consent.

4.1.3 Data minimisation

Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The data that is to be collected must be reviewed with care so that the only data collected are those which are necessary to achieve the purpose according to this principle.

4.1.4 Accuracy

Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Failure to update personal data may affect academic management or may even lead to undue disclosure of data to third parties (e.g. if the address is not kept up to date, or if the school has not correctly recorded the notification to parents concerning changes that affect the legal framework for paternal authority or custody of minors).

4.1.5 Storage limitation

Data must 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. Data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the data protection regulation in order to safeguard the rights and freedoms of the data subject.

4.1.6 Integrity and confidentiality

Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, as stipulated in section “IX”.

4.2 Information transparency

The school must be transparent regarding the data processing that is carried out, regardless of whether it is necessary to obtain the consent of the interested party or if other legal grounds apply.

For this reason, the utmost transparency must be applied in all the processing that the school carries out, so that people are aware of the use that is being made of their data at all times. For example, having a clearly visible privacy notice on institutions' websites will enable people to be informed at all times.

4.2.1 Information to the data subject

Transparency in data processing is specified very clearly in the subject's right of information both when the data is collected directly or by third parties.

When the data are collected directly from the data subject

Information can be provided to the dada subject by adopting an information model with layers or levels: giving the basic information in the first level, and providing an e-mail address or other means that provides access to the information in a simple and immediate manner.

These levels are as follows:

First level. Basic information that provides general knowledge about the processing.

- The identity of the data controller.
- The purpose of the processing.
- The ability to exercise the right to informational self-determination, the right of access, rectification, erasure and to object, as well as the right to the restriction of processing, to data portability and to challenge decisions.

Second level. Other information.

- The identity and contact details of the data controller and where applicable, their representative.
- The contact details of the data protection officer.
- The purposes and legal framework for the processing.
- The legitimate interests which are the grounds for processing, where appropriate.
- The recipients or categories of recipients of the data.
- The intention to transfer the data to another country or to an international organisation and the grounds for doing so, if applicable.
- The period during which the data will be stored, or the criteria for determining this.
- The right to request access to data, rectification or erasure of data, limitation and objection to the processing and portability of the data.
- The right to withdraw the consent that has been granted at any time.

- If the communication of data is a legal or contractual requirement or a requirement necessary to sign a contract, and whether the data subject is obliged to provide the data and the consequences of not providing them.
- The right to file a complaint with a supervisory authority.
- The existence of automated decision-making, including profiling, the logic applied and the consequences thereof.

When the data are not collected directly from the data subject

In addition to the aspects listed above, information about the following must be provided:

- The categories of personal data processed.
- The source of the data and if they are sources with public access.

4.2.2 Exceptions to the right to information

It is not necessary to inform when:

- The data are collected from the data subject and the data subject already has the information.
- The data are not collected from the data subject and any of the following circumstances apply:
  - The data subject has all the legally required information.
  - Communication is impossible or involves a disproportionate effort.
  - Obtaining or communicating the data is expressly established under European Union or Member State law.
  - The data must remain confidential due to a legal obligation of professional confidentiality, including a statutory obligation of confidentiality.

4.2.3 Where and how to provide information

The obligation to inform must be fulfilled without any request, and the data controller must subsequently be able to provide proof that this obligation has been fulfilled.

Under all circumstances, the information to data subjects must be provided:

- In clear and plain language.
- In a concise, transparent, intelligible, easily accessible and easy to understand manner.
- Balancing conciseness and precision, avoiding circumlocutions, unnecessary explanations and confusing details.

- Avoiding excessive and unnecessary legal quotations and terms that are ambiguous or lack meaning for the recipients.
- Using a language appropriate to their level of understanding, if the recipients are minors.

The information can also be provided orally if requested by the data subject.

4.2.4 At what point in the processing should the information be given?

The information must be made available to the data subjects within the following period:

- If the information is obtained from the data subject, at the time the data is collected.
- If the information is not obtained from the data subject, within a reasonable period, but in any event within a month, unless earlier notification is required because any of the following situations apply:
  - If the data must be used to communicate with the data subject, the data subject must be informed before or in the first communication with him/her.
  - If the data is to be disclosed to another recipient, the data subject must be informed when this communication takes place or beforehand.
  - If the data are subsequently to be used for a purpose other than the one for which they were collected, the necessary information related to this new purpose must be provided beforehand.

Links

You will find the Guide to compliance with the obligation to inform on the Authority's website. This provides guidelines and instructions for complying with this obligation:
Guide to compliance with the obligation to inform

Is it necessary to inform data subjects who have already been informed in accordance with the Data Protection. Law about the new aspects required by articles 13 and 14 of the GDPR?

The GDPR expands the issues regarding which data subjects must be informed, and changes some aspects relating to how this information must be provided. However, according to the stipulations of the GDPR there is no requirement to inform once again for data collected before 25 May 2018. According to the GDPR, the obligation to inform only applies to data collected after that date. However, if circumstances permit, a good practice is to use communications with data subjects to inform them of the new issues raised by the GDPR.

4.3 Legal grounds for processing personal data

Schools have to process large volumes of personal data in order to carry out their activities. The processing is only lawful if at least one of the conditions detailed below is fulfilled:

- When the data subject has given their consent.
- When it is necessary to execute a contract or apply precontractual measures.
- To fulfil a legal obligation.
- To protect the vital interests of the data subject or another natural person;
- To perform a task carried out in the public interest or in the exercise of official authority conferred on the data controller.
- To protect legitimate interests pursued by the data controller or by a third party, provided that the interests or the fundamental rights and freedoms of the data subject requiring the protection of personal data do not prevail, especially if the data subject is a child. (This paragraph does not apply to processing carried out by public authorities as part of their activities).

Processing is not permitted for special categories of data except when one of the circumstances established in the GDPR applies, such as:

- The data subject has given their explicit consent to the processing of this personal data for one or more specific purposes.
- The processing is necessary to protect the vital interests of the data subject or of another natural person, in the event that the data subject is physically or legally incapable of giving consent.
- Or other circumstances, such as when the processing involves personal data that the data subject has manifestly made public, when they are necessary for the purposes of preventive or occupational medicine, etc.

Any processing of data and therefore also the communication of data to third parties must also be based on one of the legal grounds listed above.

Some examples of communications include:

- Communications of data for academic purposes.
- Extra-academic communications.
- Communications for administrative purposes.
- Communications with public administrations.

4.3.1 Organic education law: authorisation for data processing in schools

Both publicly and privately owned schools can process their students' personal data that are necessary for performing their educational and guidance activities. This is stipulated in the

Organic Education Law, which authorises the processing of students' data for this purpose from the time when the student joins the school. The Organic Education Law also authorises the school, if necessary, to provide information about students, such as from the school where they were previously enrolled to the new school where the student is continuing his/her studies.

Likewise, the Organic Education Law authorises schools to process special categories of data, when knowledge thereof is necessary for the students' education and guidance.

For all other tasks that are not part of the school's teaching and guidance role, the legal grounds for processing must be sought (consent, contract, public interest, etc.).

4.3.2 Contractual relationship: Authorisation for teachers and workers at the school

Schools can process data relating to their workers without their consent, when these data are required to maintain or fulfil the their employment or administrative relationship with the school.

4.3.3 Consent: Services other than teaching and guidance

For other cases in which data must be processed for purposes other than teaching and guidance, such as posting photos on the school's website, or providing data to summer camps, museums or other establishments visited, consent is required from the owner of the data, or from his/her representative if the owner is a minor.

Consent must be given by a clear affirmative act of consent in which the data subject agrees to the processing of personal data by a written statement or an oral statement. This expression of consent must be:

- Freely given; the person must be able to freely refuse to have their data processed.
- Specific; the consent refers to specific processing treatments and for a specific, explicit and legitimate purpose of the controller. Generic authorisations are not permitted.
- Informed; the service must be informed beforehand of the processing, so that they are aware of its existence and purposes.
- Unambiguous; the request and the granting of the consent must take place clearly.

The GDPR requires the data subject to provide consent through an unambiguous statement or clear affirmative action for each of the purposes for which consent is requested. This means that for the purposes of the GDPR, pre-ticked boxes, tacit consent or inactivity do not constitute valid consent.

It is the data controller's responsibility to obtain the data subject's consent for specific processing.

Is it possible to continue processing based on tacit consent which began before 25 May 2018?

The GDPR stipulates that consent must consist of a clear statement or affirmative act that reflect an indication of the data subject's freely given, specific, informed and unambiguous agreement to the processing of the personal data that affects him or her. Silence, pre-ticked boxes or inactivity (e.g. tacit consent) do not therefore constitute valid consent according to the GDPR.

Accordingly, data processing based on tacit consent which began before 25 May 2018 must comply with the requirements of the GDPR before that date, either by obtaining a new consent that meets the requirements stipulated in the GDPR, or by means of any of the legal grounds established by the GDPR.

4.3.4 Consent: Minors

Schools will normally process data relating to minors. For processing that requires consent, i.e. processing that is not included in the school's teaching and guidance role, the consent of parents or guardians is required when the students are younger than 14 years old.

Students over 14 years old can give their own consent, except in cases in which the law requires the assistance of the holders of paternal authority or guardianship.

The protection of minors also involves the requirement that the information is provided in easily understandable language.

4.3.5 Consent: Networks and minors

Schools must be aware of their responsibility as regards the improper use or dissemination of the images of minors. Data protection regulations specifically regulate the protection of minors on the Internet, and stipulate that the use and distribution of images and personal information relating to minors on social networks which may entail an illegal interference in their fundamental rights will lead to intervention by the prosecution service, which may take the precautionary and protective measures established by law.

Schools, and anyone who is engaged in activities involving minors and in which their data is processed (images, voice, etc.) must guarantee the protection of the child's best interests and fundamental rights and freedoms. In this case, especially regarding the right to the protection of personal data, at the time their personal data are published or disseminated by means of information society services, the school must have the consent of the minors or

their parents or guardians before carrying out any publication or dissemination of student's data on the school's website or Intranet.

4.3.6 Withdrawal of consent

The data subject can withdraw the consent granted at any time, with no retroactive effect. The data subject must be informed of this possibility before they give their consent. It must be as easy to withdraw consent, as it is to give it.

5. Rights of the data subject

5.1 Rights of the data subject

These rights are extremely personal and must be exercised by the data subject themselves or a third party representing them before the data controller.

Holders of paternal authority may always exercise these rights on behalf of and representing children under 14 years of age.

5.1.1 Right of access

The data subject has the right to know whether the data controller is processing their personal data and if so, have access to it and to obtain the following information:

- The purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipient to whom the data have been or will be disclosed.
- The period envisaged during which the personal data will be stored, or the criteria used to determine this.
- The right to request from the controller rectification or erasure of the data, restriction of processing or to object to it.
- The right to lodge a complaint with the competent supervisory authority.
- The source of the data, when they were not obtained from the data subject.
- The existence of automated decision-making, including profiling, the logic applied and the consequences of this processing.
- In cases where data is transferred internationally, the appropriate safeguards that are provided.

The data subject has the right to obtain a copy of the data that are subject to processing free of charge. A fee for administrative costs may be charged for further copies. When the request is by electronic means, the data subject has the right to receive the information in the same format.

If requests are manifestly unfounded or excessive, especially because of their repetitive nature, the data controller can charge a reasonable fee based on the administrative costs that have been met to provide the information or the communication, or to carry out the action requested, or refuse to act on the request. The data controller must demonstrate the manifestly unfounded or excessive nature of the request.

5.1.2 Right to rectification

The data subject has the right to obtain rectification of their inaccurate personal data and to complete their incomplete personal data, including by means of a supplementary statement.

The data subject must make the request clearly and in detail, indicating the data concerned and the correction that must be made. The request must be accompanied by documentation that justifies the rectification, if applicable.

The controller must notify each recipient of the rectification, unless this is impossible or requires disproportionate efforts. The controller must identify the recipients if requested to do so by the data subject.

5.1.3 Right to erasure or right to be forgotten

Data subjects have the right to have their data erased ("the right to be forgotten") when:

- The data are no longer necessary for the purpose for which they were collected.
- The consent on which the processing was based has been withdrawn.
- The data subject opposes the processing.
- The data have been unlawfully processed.
- The data must be erased to comply with a legal obligation.
- The data were obtained in relation to the provision of information society services for minors.

When the controller has made personal data public and must erase them, the controller must take reasonable steps to inform controllers that are processing the data of the erasure.

The controller must notify each of the recipients of the erasure, unless this is impossible or requires disproportionate efforts. The controller must identify the recipients if requested to do so by the data subject.

Some exceptions to the exercise of this right are envisaged:

- Exercising the right to freedom of expression and information.
- Compliance with a legal obligation.

- The existence of archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- The establishment, exercise or defence of claims.

5.1.4 Right to restriction of processing

Restriction of processing means that at the request of the data subject, their personal data will not be subject to the processing that would apply in each case.

Restriction can be requested when:

- The data subject has exercised their rights of rectification or objection and while the controller decides whether to act on the request, if appropriate.
- The processing is unlawful, which would lead to the erasure of the data, but the data subject opposes this.
- The data are no longer required for the processing, which would again lead to their erasure, but the data subject requests restriction because he/she needs them to establish, exercise or defend claims.

While the restriction applies, the controller can only process the data affected, apart from storing them, in the following cases:

- With the data subject's consent.
- To establish, exercise or defend claims.
- To protect the rights of another natural or legal person.
- For reasons of important public interest in the European Union or in a Member State.

The controller must notify each of the recipients of the restriction, unless this is impossible or requires disproportionate efforts. The controller must identify the recipients if requested to do so by the data subject.

5.1.5 Right to data portability

The right to data portability is an advanced form of the right of access, whereby the data subject has the right to receive the personal data that affect them in a structured, commonly used and machine-readable format, if the following requirements are met:

- The processing is based on consent or a contract.
- The processing is carried out by automated means.

The data subject may ask the controller for the data that they have provided and which affect them, including data resulting from the data subject's activities.

The right to data portability includes the right to have data transmitted directly from one controller to another, if this is technically possible.

This right cannot be exercised when the processing is based on performance of a task in the public interest or in the exercise of public authority.

5.1.6 Right to object

The data subject has the right to object to the processing of their personal data:

- When the processing is based on the public interest or the exercise of public authority vested in the controller, or on the legitimate interest pursued by the data controller or by a third party. In this case, the objection must be based on grounds related to the data subject's personal situation. The data controller must cease the processing, unless the controller demonstrates compelling legitimate grounds for the processing, which override the interests of the data subject or are necessary to exercise or defend claims.
- When the processing is for statistical, scientific, or historical research purposes and grounds related to the data subject's personal situation are cited, unless the processing is necessary for performing a task in the public interest.
- When the processing is for the purposes of direct marketing, including profiling related to that marketing. The data subject can object at any time, with no need to justify their request.

5.1.7 Right not to be subject to automated individual decision-making

The data subject has the right not to be subject to a decision based solely on the automated processing of their data, including profiling, which produces legal effects concerning them or significantly affects them, unless the decision:

- Is necessary for entering into or executing a contract between the data subject and a data controller.
- Is based on the data subject's explicit consent.
- Is authorised by European Union or Member State law.

If decisions of this nature are taken, the data subject must be informed.

5.2 Exercising the rights

5.2.1 Who can exercise these rights?

The data subject or a representative on their behalf, for minors under 14 years old, disabled people, people over 14 years of age if required by law, or when the data subject voluntarily designates someone to represent them.

5.2.2 Procedure: How are the rights exercised?

- The data controller must respond to the data subject in a manner that is concise, transparent, intelligible and easily accessible, using clear and plain language, especially if the information is specifically aimed at a child.
- The controller must provide the answer in writing or by other means, including by electronic means, if appropriate. If requested by the data subject, the answer can be given orally if they prove their identity by other means.
- The data controller must facilitate the data subject's exercise of their rights, and must not refuse to act on the request of the data subject unless the controller can prove that he/she is unable to identify the data subject.
- The data controller must provide the data subject with information on actions taken, if the request was made in accordance with the GDPR and within one month of receiving the request. This period can be extended by a further two months, if necessary, taking into account the complexity and the number of requests. The controller must inform the data subject of any extension of this nature within one month of receiving the request, together with the reasons for the delay. When the data subject submits the request by electronic means, the information must be provided by those same means whenever possible, unless the data subject requests otherwise.
- The information must be provided free of charge. If the requests are manifestly unfounded or excessive, especially because of their repetitive nature, the controller may:
  - Charge a reasonable fee, taking into account the administrative costs involved in providing the information or the communication, or carrying out the action requested.
  - Refuse to act on the request.
- The controller must bear the burden of demonstrating the manifestly unfounded or excessive nature of the request.
- When the controller has reasonable doubts about the identity of the natural person making the request, they may request the additional information necessary to confirm the identity of the data subject.

5.2.3 Where must the request be submitted?

The data subject must submit the request to the data controller, which is either the school that processes their data or the Ministry.

Rights can also be exercised against the data processor. In this case, the processor (e.g. the company that provides the school meals service) must pass on the request to the controller for the latter to deal with it, except in cases where the data processor's contract enables it to deal with requests on behalf of the controller.

If the controller, or where appropriate the processor, fails to deal with the data subject's request, without delay and within one month, the data subject must be informed that their request has been received, of the reasons for the delay, and of the possibility of filing a claim before the Catalan Data Protection Authority and taking legal action.

5.2.4 Complaints concerning disregard for rights

Data subjects whose exercise of the rights of informational self-determination are partially or totally denied, or who consider that their request has been rejected because it has not been dealt with within the established period may file a complaint with the Catalan Data Protection Authority. The Authority will decide if there are grounds for the refusal or otherwise by means of a rights protection procedure.

6. The obligation of secrecy

The data controller and everyone involved in any of the phases of processing of personal data are subject to the obligation of confidentiality regarding those data. The Organic Education Law stipulates that teaching staff and other staff who, as part of their work, have access to personal and family data or data that affect the honour and privacy of minors or their families, are subject to the obligation of confidentiality.

When carrying out their activities, schools work not only with teachers, but also with various other professionals: e.g. psychologists, pedagogues, speech therapists, special needs teachers and social educators. Schools also have administrative personnel and other auxiliary services, such as maintenance and school meals staff. All of them have access to or may at some time access information or documentation systems that contain the students' personal data.

To ensure compliance with this obligation, in a legal relationship that entails the processing of personal data, the obligation must be incorporated and defined in employment contracts, internal protocols, training activities and in the specific regulations that encompass the rights

and obligations of the parties involved. This obligation continues even when the relationship with the controller has ended.

Compliance with the obligation of secrecy is particularly important in an area like education, in which information that must receive special protection may often be processed. This includes information obtained from professionals in the areas of guidance, psychologists, pedagogues, speech therapists, special needs education and social educators, and may include professional diagnostics, assessments and opinions on the students' state of physical or mental health, and assessments of their personal and family life.

7. The data protection officer

7.1 The data protection officer in schools

Schools are required to appoint a data protection officer (DPO). This obligation also extends to the state-assisted and private schools, according to the draft Organic Law for the Protection of Personal Data, published in the Official Bulletin of the Spanish Parliament number 13-1, of 24 November 2017.

The data protection officer may be a member of staff or work basis of a contract. A school's data protection officer can act as the officer of other schools, or several schools may have the same officer for all of them.

Schools must publish the contact details of the data protection officer and notify the Catalan Data Protection Authority of the designations, appointments and revocations of appointments of their data protection officer within 10 days.

The data protection officer has the following tasks, among others:

- To inform and advise the school or the processor and the employees on the obligations pursuant to the data protection regulations.
- To monitor compliance with the regulations.
- To provide advice on the data protection impact assessment.
- To act as the school's contact point with the data protection Authority.

The position of the DPO in organisations must meet the requirements expressly set out in the GDPR. These requirements include total autonomy when performing his/her tasks, the need for relations with senior management and the obligation that the controller or processor provides them with all the necessary resources to carry out the activities.

7.2 What requirements or qualifications must the data protection officer fulfil?

The DPO must be appointed taking into account their professional qualifications and in particular, their knowledge of data protection legislation and practice. This does not mean that the DPO requires a specific qualification. Bearing in mind that their tasks include advising the controller and the processor on everything related to data protection regulations, legal knowledge in this area is undoubtedly necessary; but knowledge beyond the strictly legal sphere is also required, e.g. in the field of technology applied to data processing or related to the area of activity of the organisation in which the officer works.

8. The data protection impact assessment

When processing is likely to entail a high risk for individuals' rights and freedoms, due to its nature, scope, context or purposes, especially if new technologies are used, the controller should carry out a data protection impact assessment prior to the processing.

8.1 How is the need to carry out an impact assessment determined, and what must it contain?

The GDPR contains a list of recommendations with three cases in which processing is considered to involve a high risk:

- Profiling based on which decisions are made that have legal effects on the data subjects or a significant effect in a similar manner.
- Large-scale processing of special categories of data.
- Systematic observation of a publicly accessible area on a large scale.

In the guidelines on Data Protection Impact Assessment (DPIA) (WP248), the Article 29 working party considers that in order to assess what constitutes largescale processing treatment, the following factors should be taken into account:

- The number of data subjects involved, either in absolute terms or as a proportion of a specific population.
- The volume and variety of data processed.
- The duration or permanence of the processing activity.
- The geographical extent of the treatment activity.

Links

The Catalan Data Protection Authority impact assessment guide (DPIA) should be consulted when establishing the concept of high risk for the purposes of the requirement to conduct an impact assessment and the criteria for doing so.
Data protection impact assessment guide

What happens with processing that began before 25 May 2018, for which the data protection impact assessment (DPIA) is required according to the new regulations?

If this processing continues after 25 May 2018 and the risk analysis that organisations carry out for processing that began prior to that date shows that this processing entails a high risk to the rights or freedoms of the data subjects, the data protection impact assessment Guide also recommends carrying out a DPIA.

8.2 Prior consultation

In cases where the DPIA identifies a high risk which in the opinion of the processor cannot be mitigated by reasonable means in terms of the technology available and costs of application, the controller must consult the Catalan Data Protection Authority. The consultation must be accompanied by the documentation provided by the GDPR, including the impact assessment itself.

Links

To request a prior consultation, follow the steps listed in our online office:
Prior consultation

The Catalan Data Protection Authority must give written advice to the data controller and, if necessary, to the processor, and may use all the powers conferred by the Regulation, including prohibition of the processing.

9. Security measures

Unlike the current regulations, the Regulation does not establish a list of security measures that are applicable according to the type of data being processed, but instead stipulates that the data controller and data processor must apply technical and organisational measures appropriate to the risk involved in the processing. This implies having to assess the risks

involved in each processing in order to determine the security measures that must be implemented.

9.1 How is a risk analysis performed?

From the point of view of information security, a risk analysis requires an identification of threats (e.g. unauthorised access to personal data), an assessment of the probability of their occurrence, and the impact they would have on the data subjects.

The type of analysis varies according to:

- The types of processing.
- The nature of the data being processed.
- The number of people affected.
- The amount and variety of processing carried out by the organisation.
- The technologies used.

As a general rule, in large organisations, this risk analysis and determination of the measures or checks to be implemented can be carried out using any of the existing risk analysis methodologies or standards: e.g. MAGERIT, ISO, etc. For controllers with smaller dimensions and with little complexity, this analysis can be the result of a documented reflection on the implications of processing on the rights and freedoms of the data subjects. This consideration must examine the context in which the processing is carried out (means, facilities, users, etc.) and must answer questions such as the following:

- Are special categories of data processed?
- Are data from vulnerable groups (e.g. minors) processed?
- Are data from a large number of people processed?
- Can the data processed enable profiling?
- Can the disclosure, alteration or loss of data have significant consequences for the data subjects?
- Are the data processed outside the control's equipment or facilities?
- Do third parties providing services on behalf of the controller have access to the data?
- Are technologies used that are particularly invasive of privacy (geolocation, video surveillance, Internet of Things, etc.)?

There are many issues that can impact negatively on the rights and freedoms of people if data are not processed correctly. It is therefore very important that if a standard, easily auditable and objective methodology is not used, the issues that have been taken into account when determining the level of existing risk and specifying the measures of security to be applied must be documented. This will enable compliance with the accountability principle.

However, the more questions are answered in the affirmative, the greater the risk involved in the processing.

Does this change in focus in the GDPR mean that the measures that an institution applied following the Data Protection Law Regulations are not correct?

No. Perhaps they are appropriate, but in any case, the risk analysis must be performed to determine whether the measures implemented are correct or if there is any shortcoming.

In any event, the specific measures to apply must guarantee:

- The ongoing confidentiality, integrity, availability and resilience of the processing systems and services.
- The ability to restore the availability and access to personal data quickly in the event of a physical or technical incident.
- The existence of a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures established to guarantee the security of the processing.

Can the security measures stipulated in the Data Protection Law Regulations continue to be applied?

The GDPR does not establish a list of security measures based on basic, medium and high security levels, as the Data Protection Law Regulations did. It leaves the security measures to be implemented in each case to the discretion of the controller and processor, after assessment of the risks.

In any event, the appropriate technical and organisational safety measures must be adopted to ensure a level of protection that is appropriate to the risk. The measures provided for in the Data Protection Law Regulations that are already in place may be useful, but it is necessary to assess whether they are sufficient or if they need to be modified in each case.

9.2 Notification of data breaches

Personal data breaches: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Situations such as the loss or theft of a laptop computer, unauthorised access to the database (even by the school's staff), sending personal information to an incorrect recipient, the unauthorised alteration of data or the loss of data availability (e.g. due to having suffered an attack on systems with hijacking software or ransomware, which encrypts the data)

constitute data breaches, and they must be dealt with in accordance with the provisions of articles 33 and 34 of the GDPR.

In the event of a personal data breach, the controller must, without undue delay and, where feasible, within 72 hours, 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 (art. 33. GDPR).

In addition, when the data breach is likely to result in a high risk to the rights of natural persons, the controller must inform the data subject without undue delay, unless:

- The controller has taken appropriate protection measures, such as rendering the data unintelligible to unauthorised persons.
- The controller has taken subsequent measures which ensure that the high risk is no longer likely to materialise.
- It would involve disproportionate effort (art. 34. GDPR).

9.2.1 What is the deadline for notifying a data breach to the supervisory Authority?

The data breach must be notified to the authorities without undue delay and if possible, within 72 hours after the controller has become aware of it. This criterion may be subject to various interpretations. In general, a security breach is considered to have taken place when there is reasonable certainty that there a security incident has occurred that has compromised personal data and there is sufficient knowledge of its nature and extent. Notification should not take place if a breach is simply suspected to have occurred, without any knowledge of the circumstances, as in most cases, under these conditions it is not possible to determine the extent to which there may be a risk to the rights and freedoms of the data subjects affected.

However, in cases of breaches that may have a considerable impact due to their characteristics, it may be advisable to contact the supervisory authority as soon as there is evidence that an irregular situation has arisen regarding the security of the data. Notwithstanding the above, these first contacts may be complemented by a formal, more comprehensive notification within the legally envisaged period.

If the notification to the supervisory authority does not occur within 72 hours, it must be accompanied by an explanation of the reasons that caused the delay.

9.2.2 What must the notification of a personal data breach to the supervisory Authority contain?

The notification must contain some minimum details stipulated in the GDPR (art. 33 GDPR), which includes the nature of the breach, the categories and approximate number of data affected, the measures taken by the controller to address the breach and where appropriate, the measures taken to mitigate the possible negative effects on the data subjects affected.

If it is not possible to provide all the information at the same time, it can be provided gradually, without undue delay.

Links

When reporting a security breach, you must follow the steps listed in our electronic office or on the APDCAT website:

- In the APDCAT office
- On the APDCAT website

Irrespective of the notification to the authorities, the data controllers must document all security breaches. This is an obligation stipulated by the GDPR, which is very similar to the incident record stipulated in the Data Protection Organic Law Regulations.

9.2.3 When is a personal data breach likely to entail a high risk for the rights of the data subjects?

The high risk criterion mentioned in the GDPR must be understood in terms of the security breach being likely to cause significant damage to the data subjects. For example, this may be the case if confidential information is revealed, such as passwords or participation in certain activities, if sensitive information is disclosed or if it may entail financial damages to the data subjects.

9.2.4 What is the legal framework for notifying those affected by a personal data breach?

The purpose of this notification is to enable the data subjects affected to take steps to protect themselves from the consequences of the security breach. For this reason, according to the GDPR they must be notified without undue delay, without reference to either when the breach was recorded or the possibility of performing the notification within a period of 72 hours. The purpose is always for the data subject affected to be able to react as soon as possible.

For the same reasons, the GDPR adds to the content of the notification that, if necessary, recommendations must be established regarding the measures that can be taken by the data subject affected in order to deal with the consequences of the breach.

9.2.5 What could happen if a personal data breach is not notified?

If a security breach is not notified to the supervisory authority, this may constitute an infringement of an obligation stipulated in the GDPR, unless it is unlikely that the breach entails a risk to the rights and freedoms of natural persons.

Failure to provide notification of the data security breach within 72 hours if there are no reasons to justify this may also constitute an infringement of the GDPR. These infringements may lead to the exercise of investigative and corrective powers, including the imposition of a fine, if necessary.

However, there is no penalty if the authority is notified of a security incident that is not considered a security breach of personal data with mandatory notification.