**General Data Protection Regulation (GDPR) - Information for Colleges and EBVS**

**What is GDPR?**

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on **data protection and privacy for all individuals within the European Union**. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

It was adopted on 14 April 2016, and after a two-year transition period, becomes enforceable on **25 May 2018**. The GDPR replaces the 1995 Data Protection Directive. Because the **GDPR is a regulation**, not a directive, it does not require national governments to pass any enabling legislation and is **directly binding and applicable**.

**Who is affected by GDPR?**

**We are.** The regulation applies if the **data controller** (an organisation that collects data from EU residents i.e. an EBVS college), or **processor** (an organisation that processes data on behalf of a data controller i.e. the EBVS on behalf of the college), or the **data subject** (person i.e. the college members) is based in the EU.

**Who’s responsibility is it to comply with GDPR?**

It is the **responsibility and the liability of the data controller** (i.e. the colleges) t**o implement effective measures and be able to demonstrate the compliance** of processing activities, even if the processing is carried out by a data processor on behalf of the controller (i.e. EBVS) (Recital 74).

To be able to demonstrate compliance with the GDPR, the data controller should **implement measures**, which meet the principles of data protection by design and data protection by default. Such measures could consist of **minimising the processing of personal data**, **pseudonymising** personal data as soon as possible, **transparency** with regard to the functions and processing of personal data, **enabling the data subject to monitor the data processing**, enabling the controller to **create and improve security features**. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. (Recital 78)

Under the GDPR, personal data must be processed following principles so that the data are:

* + Processed fairly, lawfully and transparently and only if there is a valid 'legal basis' for doing so
  + Processed only for specified, explicit and legitimate purposes
  + Adequate, relevant and limited
  + Accurate (and rectified if inaccurate)
  + Not kept for longer than necessary
  + Processed securely to preserve confidentiality, integrity and availability of the personal data

**What is personal data?**

Any **information relating to an identified or identifiable person** (‘data subject’ i.e. the college members). These ‘data subjects’ can be identified, directly or indirectly, by 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 person.

**When are we allowed to process personal data?**

Data may not be processed unless there is at least one lawful basis to do so (see also Article 6 in Annex 1):

* + - **The data subject has given consent to the processing of personal data for one or more specific purposes.**
    - 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.
    - Processing is necessary for compliance with a legal obligation to which the controller is subject.
    - Processing is necessary to protect the vital interests of the data subject or of another person.
    - 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.
    - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular if the data subject is a child.

It is possible that EBVS and colleges may actually fall under one of the other ‘lawful bases’, however it is prudent to assume that **we will at least need consent from our members**.

**How do we obtain consent?**

Where processing is based on consent, the controller shall be able to **demonstrate that the data subject has consented** to processing of his or her personal data (Article 7).

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 has the right to **withdraw his or her consent at any time**. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It should be as easy to withdraw as to give consent.

As the diplomate status will be affected by the diplomates willingness to share their personal data, it will be difficult to comply with recital 42: Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Losing diplomat status would certainly be a detriment, however it is impossible for us to impart this status without personal data. The consent is formulated in such a way that it does not threaten the data subject with loss of their specialist status; we can assume that they understand this.

**Other than consent, what should we do to comply?**

Associations or other bodies representing categories of controllers or processors (i.e. EBVS) should be encouraged to draw up **codes of conduct,** within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of the data subjects. This means we have an **obligation to draft official EBVS policy documents on data protection**. This will be done by the EBVS and a template will be circulated to colleges.

**Do we need a data protection officer?**

If the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity or if, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects at a large scale, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this regulation.

The DPO is similar to a compliance officer and is also expected to be proficient at managing IT processes, data security (including dealing with cyberattacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations.

As our *core* activities do not consist of ‘processing operations that require regular and systematic monitoring of the data subjects *at a large scale’* it would appear that such a role would be beyond the scope of the EBVS colleges. The liability is primarily with the colleges (as data controllers) meaning that the scale of the operations is very small (800 max). We can therefore **assume that we will not need a DPO.** Queries to FVE and EAEVE that work on a larger scale than EBVS show that they have reached the same conclusion.

More information on the DPO’s can be found in this guideline document

<http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>.

**What happens if we do not comply?**

The following sanctions can be imposed:

* a warning in writing in cases of first and non-intentional noncompliance
* regular periodic data protection audits
* a fine *up to* €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater

Although it is likely that organisations such as EBVS or its colleges will not be the first to come under scrutiny, we must make every effort to ensure we are compliant. The conditions for fines depend on the circumstances and we should be able to provide evidence that we have done our utmost to comply (Article 83).

**ANNEX 1**

Although we strongly encourage everyone to read through the full GDPR (available at: <https://gdpr-info.eu/>), to save time, the articles that are believed to be of most relevance to EBVS and colleges are included this annex: 4 (Definitions) 5 (Principles relating to processing of personal data), 6 (Lawfulness of processing), 7 (Conditions for consent) 11 (Processing which does not require identification), 13 (Information to be provided where personal data are collected from the data subject), 17 (Right to erasure), and 34 (Communication of a personal data breach to the data subject).

**Art. 4 GDPR**

**Definitions**

For the purposes of this Regulation:

1. ‘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;
2. ‘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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
4. ‘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 analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. ‘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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
7. ‘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;
8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. 1‘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. 2However, 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;
10. ‘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 authorised to process personal data;
11. ‘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;
12. ‘personal data breach’ means 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;
13. ‘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;
14. ‘biometric data’ means 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;
15. ‘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;
16. ‘main establishment’ means:
    1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
    2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
17. ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to [Article 27](https://gdpr-info.eu/art-27-gdpr/), represents the controller or processor with regard to their respective obligations under this Regulation;
18. ‘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;
19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;
20. ‘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;
21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to [Article 51](https://gdpr-info.eu/art-51-gdpr/);
22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:
    1. the controller or processor is established on the territory of the Member State of that supervisory authority;
    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
    3. a complaint has been lodged with that supervisory authority;
23. ‘cross-border processing’ means either:
    1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
    2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
24. ‘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;
25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of [Directive (EU) 2015/1535](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535) of the European Parliament and of the Council (¹);
26. ‘international organisation’ means an organisation 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.

**Art. 5 GDPR**

**Principles relating to processing of personal data**

1. Personal data shall be:
   1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
   3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
   4. 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 (‘accuracy’);
   5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
   6. 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 (‘integrity and confidentiality’).
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

**Art. 6 GDPR**

**Lawfulness of processing**

1. 1Processing shall be lawful only if and to the extent that at least one of the following applies:
   * 1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
     2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
     3. processing is necessary for compliance with a legal obligation to which the controller is subject;
     4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
     5. 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;
     6. 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.
2. 2Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
3. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in [Chapter IX](https://gdpr-info.eu/chapter-9/).
4. 1The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
   * 1. Union law; or
     2. Member State law to which the controller is subject.
5. 2The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 3That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in [Chapter IX](https://gdpr-info.eu/chapter-9). 4The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.
6. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in [Article 23](https://gdpr-info.eu/art-23-gdpr/)(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
   * 1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
     2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
     3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to [Article 9](https://gdpr-info.eu/art-9-gdpr/), or whether personal data related to criminal convictions and offences are processed, pursuant to [Article 10](https://gdpr-info.eu/art-10-gdpr/);
     4. the possible consequences of the intended further processing for data subjects;
     5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

**Art. 7 GDPR**

**Conditions for consent**

* Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
* 1If 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. 2Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
* 1The data subject shall have the right to withdraw his or her consent at any time. 2The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 3Prior to giving consent, the data subject shall be informed thereof. 4It shall be as easy to withdraw as to give consent.
* When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

**Art. 11 GDPR**

**Processing which does not require identification**

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. 1Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. 2In such cases, [Articles 15](https://gdpr-info.eu/art-15-gdpr/) to [20](https://gdpr-info.eu/art-20-gdpr/) shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

**Art. 13 GDPR**

**Information to be provided where personal data are collected from the data subject**

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
   1. the identity and the contact details of the controller and, where applicable, of the controller’s representative;
   2. the contact details of the data protection officer, where applicable;
   3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   4. where the processing is based on point (f) of [Article 6](https://gdpr-info.eu/art-6-gdpr/)(1), the legitimate interests pursued by the controller or by a third party;
   5. the recipients or categories of recipients of the personal data, if any;
   6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in [Article 46](https://gdpr-info.eu/art-46-gdpr/) or [47](https://gdpr-info.eu/art-47-gdpr/), or the second subparagraph of [Article 49(](https://gdpr-info.eu/art-49-gdpr/)1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
   1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
   2. 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;
   3. where the processing is based on point (a) of [Article 6](https://gdpr-info.eu/art-6-gdpr/)(1) or point (a) of [Article 9(](https://gdpr-info.eu/art-9-gdpr/)2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
   4. the right to lodge a complaint with a supervisory authority;
   5. 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;
   6. the existence of automated decision-making, including profiling, referred to in [Article 22](https://gdpr-info.eu/art-22-gdpr/)(1) and (4) 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.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

**Art. 17 GDPR**

**Right to erasure (‘right to be forgotten’)**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
   1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   2. the data subject withdraws consent on which the processing is based according to point (a) of [Article 6](https://gdpr-info.eu/art-6-gdpr/)(1), or point (a) of [Article 9](https://gdpr-info.eu/art-9-gdpr/)(2), and where there is no other legal ground for the processing;
   3. the data subject objects to the processing pursuant to [Article 21](https://gdpr-info.eu/art-21-gdpr/)(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to [Article 21](https://gdpr-info.eu/art-21-gdpr/)(2);
   4. the personal data have been unlawfully processed;
   5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
   6. the personal data have been collected in relation to the offer of information society services referred to in [Article 8](https://gdpr-info.eu/art-8-gdpr/)(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
   1. for exercising the right of freedom of expression and information;
   2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of [Article 9](https://gdpr-info.eu/art-9-gdpr/)(2) as well as [Article 9](https://gdpr-info.eu/art-9-gdpr/)(3);
   4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
   5. for the establishment, exercise or defence of legal claims.

**Art. 34 GDPR**

**Communication of a personal data breach to the data subject**

1. 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.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of [Article 33](https://gdpr-info.eu/art-33-gdpr/)(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   1. the controller has implemented appropriate technical and organisational 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 authorised to access it, such as encryption;
   2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
   3. 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.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.