

## INFORMATION SUBJECT TO THE NOTIFICATION OBLIGATION

An asterisk (\*) indicates new information that was not required by the Personal Data Act.

In addition to this information, data subjects must be clearly notified of the risks to their rights and freedoms, as provided for by recital 39 of the GDPR.

Information required by the notification obligation	Article and section: When the personal data is collected directly from the data subject	Article and section: When the data was not obtained from the data subject	Article 29 Working Party's comments on the notification obligation
The identity and contact details of the controller and its possible representative (Article 4(17))	13.1(a)	14.1(a)	The information should make it easy to identify the controller and provide a method, or preferably several methods, of contacting the controller (e.g. telephone number and e-mail and postal addresses)
Contact details of the Data Protection Officer, if any*	13.1(b)	14.1(b)	If a Data Protection Officer has been designated, his or her contact details must be provided in the information. For more information, please refer to the Article 29 Working Party's guideline on Data Protection Officers (WP 243 rev.01).
Purposes of processing personal data and the legal basis for the processing*	13.1(c)	14.1(c)	Data subjects should be made aware of the purposes for which their personal data will be processed and the section of Articles 6 or 9 on which the processing is based.
If the processing is based on legitimate interest (6.1(f), legitimate interests pursued by the controller or a third party*	13.1(d)	14.2(b)	The legitimate interests must be identified and specified. For the promotion of good processing practice, the controller should provide data subjects with preliminary information on the balance test required for invoking Article 6.1.f as a legal basis for processing. For more information, please refer to the Article 29 Working Party's guideline 06/2014.
Categories of personal data involved	–	14.1(d)	If the personal data was not obtained from the data subject (Article 14), the controller should notify the data subject of the categories of personal data to be processed, because he or she will not be aware of which of his or her personal data the controller processes.
Recipients or categories of recipients of personal data*	13.1(e).	14.1(e)	The concept of "recipient" is defined in Article 4.9 to include more than just third parties. In other words, controllers, joint controllers and processors to whom personal data is transferred or disclosed are "recipients" by virtue of the Article, and information on these recipients should be provided in addition to information on third-party recipients.

			According to the principle of fairness, the controller should primarily provide the information of the actual (named) recipient of the personal data. If the controller only provides information on categories of recipients, it must be able to demonstrate why this method is suitable. In such cases, the information on the categories of recipients should be as precise as possible and include the type (e.g. by referring to the processing activities carried out by the recipient), industry, sector, subsector and place of establishment of the recipients.
Information on the transfer of data to third countries and the safeguards employed (including the existence or absence of a Commission decision on the adequacy of data protection) and the methods for obtaining a copy or description of their contents.	13.1(f)	14.1(f)	In particular, information on the Article of the GDPR that permits the transfer of the data and the corresponding mechanism (e.g. the Commission decision referred to in Article 45 / the binding corporate rules referred to in Article 47 / the standard data protection clauses referred to in Article 46.2 / the exceptions and safeguards referred to in Article 49) should be provided. If possible, the information should include a link to the mechanism employed or information on where and how the information concerning the document in question can be obtained.
The storage time of personal data or, if this is not possible, the criteria for defining the storage time*	13.2(a)	14.2(a)	This is linked to the principles of minimisation of data (Article 5.1.c.) and storage limitation (5.1.e). The storage time (or the criteria for its definition) can be derived from mandatory (statutory) storage times or the industry's code of practice. The essential thing is to define the storage time in a manner that enables the data subject to evaluate, from his or her perspective, the storage time of specific data or data processed for specific purposes. Stating that the personal data will be stored for as long as required to achieve certain legal purposes will not suffice. Different storage times should be defined for different categories of personal data and/or purposes of processing on a case-by-case basis. In certain cases, this also includes archiving in the public interest.
Rights of the data subject <ul style="list-style-type: none"> <li>• Right of access</li> <li>• Right to rectification</li> <li>• Right to erasure</li> <li>• Right to restriction of processing</li> <li>• Right to object</li> <li>• Right to data portability</li> </ul>	13.2(b)	14.2(c)	This information should include a summary of the rights involved in the processing and how they can be exercised by the data subject. In particular, the data subject must be specifically made aware of the right to object, which must be presented clearly and separately from other information. For more information on the right to data portability, please refer to the Article 29 Working Party's guidelines on

			the right to data portability (WP 242 rev.01).
If the processing is based on consent as provided for in Article 6.1.a (or explicit consent, Article 9.2.a), information on the right to withdraw the consent at any time*	13.2(c)	14.2(d)	This information should include details on how the consent can be withdrawn, taking into consideration that withdrawing consent should be as easy as giving it (Article 7.3).
Right to lodge a complaint with a supervisory authority*	13.2(d)	14.2(e)	In this context, it should be explained to the data subject that Article 77 gives every data subject the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement of the GDPR.
Is providing the personal data a statutory or contractual requirement or a requirement for concluding a contract, and whether the data subject is obliged to provide the data, along with the possible consequences of not providing the data*	13.2(e)	–	For example, an employee may be contractually required to provide certain data to his or her current or future employer. Online forms should clearly indicate which data is mandatory and the possible consequences of not providing the data. Correspondingly, data that is not mandatory from this perspective should be indicated in an equally clear manner.
Information on the source of the personal data and, if necessary, whether the source was public or not*	–	14.2(f)	The delivered information should indicate the nature of the sources of data (e.g. whether the source was public or private, the type of the organisation/industry/sector, and the origin of the data (e.g. EU or non-EU). As a rule, the specific source of data should be stated if possible.
Information on automated decision-making, including profiling, and information relevant to the processing logic, the significance of the processing and its potential consequences for the data subject	13.2(f)	14.2(g)	For further information, please refer to the Article 29 Working Party's guidelines on automated individual decision-making and profiling (WP 251 rev.01).