

Data Protection Policy

Farnell - Data protection policy

I. Introduction

element14 (also referred to as 'Farnell', 'we', 'us' or 'our' in this Statement) is a member of a world-wide group of companies of which AVNET Inc. (based in the USA) is the parent company. We are committed to ensure compliance with applicable data protection laws and regulations. This Data Protection Policy ("Policy") is based on the principles and requirements of the EU General Data Protection Regulation ("GDPR"). By means of this Policy we would like to inform you, the data subject, about how and why we collect, process and use personal data, and about your rights as a data subject in regard to the processing of your personal data.

II. Scope and Supplement

This Policy applies to all companies, dependent group companies, affiliated companies, offices and business units of all AVNET Inc. group companies in EMEA. This Policy covers all forms of processing of personal data. It describes how Farnell collects, uses, and shares personal data obtained directly from the user, customer, supplier, business partner, or other, or obtained indirectly from other sources. It applies to the processing of personal data obtained through any channel of communication or by any means, including but not limited to email, file transfer, feeding personal data into applications and tools, websites or mobile apps, social media pages and platforms.

This Policy may be supplemented by specific data protection and privacy notices and statements that relate to specific forms or purposes of data processing. Anonymised data (non-personal data), e.g. for statistical evaluations or studies, is not subject to this Policy.

In countries where the data of legal entities is protected to the same extent as personal data, this Policy applies equally to data of legal entities.

III. Application of national laws

While the GDPR is applicable throughout the EU, there may be laws and regulations in some countries which specify further data protection requirements, in particular conditions for lawful data processing. If so, it has to be verified on a case-to-case basis whether these laws can prevail.

IV. Glossary and definitions

A glossary of specified terms and definitions shall be included in Appendix A to this Policy.

V. Personal Data we process, Purposes and Legal Basis

This section of our Policy describes what personal data we collect and process and for what purposes and on what legal basis. The amount of personal data we process depends on the context and circumstances of your interaction with us.

1. Handling orders and fulfilling contractual obligations

When you place orders to purchase goods or services from us, or if you request information about products and services prior to placing an order, or if you request support regarding the

product or services you have ordered, we will process personal data that is necessary to negotiate and execute a contract and to fulfil any contractual obligations, and to exercise our rights under the contract. This also includes advisory services under the contract if this is related to the contractual purpose. Prior to the conclusion of a contract personal data can be processed to prepare bids or tenders or to fulfil other requests of the prospect that relate to contract conclusion.

For this purpose we process **personal details** (including name, title, email, telephone, postal address, shipping and billing address), **order and customer information** (including goods and services ordered and provided, instructions regarding the order, customer business activities and interests and order history), **financial information** (including invoice data, preferred payment options, term of payment, bank account and credit card information).

The legal basis for processing personal data for the purpose of handling orders and fulfilling contractual obligations and exercising contractual rights is Article 6 (1) b) GDPR (contractual necessity). The legal basis for processing personal data for the purposes of understanding customer business activities and interests and order history is Article 6 (1) f) GDPR (legitimate interests). The legal basis for processing and keeping personal data for the purpose of complying with record keeping obligations (including commercial accounting standards and tax and fiscal retention obligations) is Article 6 (1) c) GDPR (legal obligation).

2. Browsing or registering on our websites, social media pages or platforms

When you browse our websites, social media pages or platforms, we may use Cookies and other tracking technologies to capture and understand how you use our websites, social media pages and platforms.

Not all of our websites employ Cookies and tracking technology that collect personal data. Depending on the Cookies and tracking technologies in use, we collect **information about your online browsing behaviour** on our websites, social media page or platform, including information how react to adverts and offers. We may also collect information about the device you have used to access our websites, social media pages or platforms, (including device model and operating system, browser type, IP-address, mobile device identifiers).

Specific information regarding the Cookies and tracking technology in use on our respective websites, social media pages and platforms is being provided in our [Cookie Policy](#). This includes information how to disable Cookies in your browser and how to prevent tracking of your browsing behaviour.

When you register on one of our websites, social media pages or platforms we will additionally process **personal details** (including name, title, email, telephone), and **account details** (including username, password, login-/logoff data), except where registration under an alias or pseudonym is permitted. If you decide not to provide us with this information, you may unfortunately not be able to register or use any/some of our services which require a registration.

The legal basis for processing information about online browsing behaviour, if it contains personal data, is Article 6 (1) a) GDPR (consent), if we ask you to provide consent and to agree to the processing of your personal data. Specific other provisions in laws relating to data processing in an online context may require your consent as well. Under some circumstances e.g. when we process a limited amount of personal data which, by type and nature does not significantly affect your rights and freedoms, the legal basis for processing your personal data in the context of your browsing or registering on our websites, social media pages or platforms is Article 6 (1) f) GDPR (legitimate interests).

3. Communication, marketing, taking part in promotions, events and feedback

When you contact us for any sort of inquiry or request, we will process your **personal details** (including name, title, company or organisation you work for, email, telephone, other contact information), as far as this is necessary to deal with your inquiry or request and to respond to.

When you have purchased goods or services from us, or if you have indicated to us that you are interested in certain goods or services, we may process your **personal details** (including name, title, company or organisation you work for, email, telephone, other contact information) to contact you and to send you information about our or our business partners' goods and services, new technological developments, special offers and business opportunities.

When you take part in promotions or events hosted or sponsored by us, we will process your **personal details** (including name, title, company or organisation you work for, email, telephone, other contact information) to manage your participation in the promotion or event, to provide you with information about our or our business partners' goods and services, new technological developments, special offers and business opportunities. We will also process your personal details to ask for your feedback regarding the promotion or event, your satisfaction with our or our business partners' goods or services and performance. We may also ask you for contributions to improve and enhance our goods and services and collaboration with our business partners.

The legal basis for processing personal data for the purpose of communicating with you and to respond to any sort of inquiry or request is Article 6 (1) b) GDPR (contractual necessity), as far as it occurs in the context of preparing or facilitating the conclusion of a contract or to answer to inquiries and requests in connection with a contract. As far as personal data is processed for communicating with you on other matters the legal basis is Article 6 (1) f) GDPR (legitimate interests).

When we process personal data to contact you and to send you information about our or our business partners' goods and services, new technological developments, special offers and business opportunities the legal basis is Article 6 (1) a) GDPR (consent) if we ask you to provide consent and to agree to the processing of your personal data for that purpose. Under some circumstances e.g. when we process a limited amount of personal data which, by type and nature does not significantly affect your rights and freedoms, the legal basis for processing your personal data to contact you and to send you information about our similar goods and services, new technological developments, special offers and business opportunities is Article 6 (1) f) GDPR (legitimate interests).

When we process personal data to manage your participation in a promotion or event, or to provide you with information about our or our business partners' goods and services, new technological developments, special offers and business opportunities, or to ask for your feedback or for contributions, the legal basis is Article 6 (1) a) GDPR (consent) if we ask you to provide consent and to agree to the processing of your personal data for that purpose. Under some circumstances e.g. when we process a limited amount of personal data which, by type and nature does not significantly affect your rights and freedoms, the legal basis for processing your personal data is Article 6 (1) f) GDPR (legitimate interests).

4. Legal obligations and compliance

As a business operating globally we are subject to various laws and regulations that impose legal obligations on us. Some of these laws and regulations may require the collection and processing of personal data (e.g. tax laws, commercial laws, trade and export compliance regulations, customs codes, anti-money-laundering laws). Where such legal obligations are based on EU or EU Member State laws and regulations, the legal basis for processing personal data is Article 6 (1) c) GDPR. Where such legal obligations are based on laws and regulations of third countries (non-EU), compliance with these legal obligations may represent a legitimate interest. If so, the legal basis for processing personal data is Article 6 (1) f) GDPR. The latter applies also to the processing of personal data for the purpose of ensuring compliance with our policies, codes of conduct and regulations.

5. Recruitment and application

When we recruit people we will process the personal data that you provide as part of your application. Data processing for the purpose of recruitment and carrying out the application process will generally comprise **personal details** (including name, title, email, telephone, postal address) and **CV and qualification data** (including graduation, university degree, training certificates, advanced education certificates, credentials, and skills). After completion of an application process we may continue to process (store) personal data of applicants for a certain period of time where necessary to ensure we are able to exercise rights or defend against claims in the context of the recruitment process.

The legal basis for processing personal data for the purpose of recruitment and handling applications is Article 6 (1) b) GDPR (contractual necessity), as far as the processing is necessary to review and assess the applications and to select applicants and execute an employment contract, and to exercise rights or defend against claims in the context of the applications process.

When applying for a position at Farnell via a careers website, recruitment platform or job portal, or when responding to a job advertisement, applicants should also refer further to more specific privacy information which might be made available on the careers website, recruitment platform, job portal or in the job advertisement.

VI. Personal Data of Children

Farnell's operations are focused on business-to-business (B2B). Therefore, we do not intentionally solicit personal data from children or send them requests for personal data. While users of all ages may navigate through our websites, social media pages or platforms, they are for B2B purposes only and are not targeting children. If we notice, following a notification by a parent or guardian, or after discovery by other means, that a child under 16 years has been inappropriately registered on one of our websites, social media pages or platforms, we will cancel the account and registration and delete the child's personal data from our records.

VII. Sharing Personal Data with Service Providers and Third Parties

Not all processing of your personal data will be carried out by Farnell itself. Sometimes we will make use of service providers and vendors ("processors") who will process personal data for us, on our behalf and under our instructions. Such processors can be external companies or affiliates of Farnell (group companies). Any such outsourcing of data processing will follow a service provider / vendor due diligence and monitoring protocol, and will be governed by a Data Processing Agreement.

As far as we use service providers and vendors as processors to process personal data on our behalf, your personal data may be shared with the following categories of recipients:

IT service providers, application service providers, Internet service providers, platform and website host service providers, data disposal companies, marketing agencies, market research agencies, advertising partners, order and account management service providers, payment service providers, logistics service providers, customer care service providers.

Apart from sharing personal data with service providers and vendors it may be necessary to share your personal information with third parties, because there is a legal obligation to do so, or because there is a legitimate interest to ensure compliance with policies and regulations, or to facilitate business cooperation and collaboration. In such cases your personal data may be shared with the following categories of recipients:

Public authorities and administrative bodies, law enforcement and fraud prevention agencies, courts, lawyers, tax accountants, accounting and auditing firms, credit reference agencies, payment card and insurance providers, manufacturers and resellers, retailers.

If you use our websites, social media pages or platforms and if you choose to link your social media accounts to us or if you are logged in into your social media account, your personal data may be shared with the operators of those social media pages and platforms.

Where you have been asked to sign up for the [element14 Community Site](#), with your consent your information will be passed to our UK based group company Premier Farnell Ltd as operators of that site and such data will be passed to them and they will operate as data controllers for use of your information on that site in accordance with their privacy policy.

If we sell or buy any business or assets or transfer an area of our business to a new owner, we will disclose your personal data to the prospective seller or buyer of such business or assets or any third party who acquires our assets or who the business is transferred to.

We may share information with affiliated or unaffiliated third parties on an anonymous, aggregate basis. While this information will not identify you personally and insofar not contain personal data, in some instances these third parties may be able to combine this aggregate information with other data they have about you, or that they have collected from you or received from third parties, in a manner that allows them to identify you personally. Where we do share such data with third parties, we take steps to ensure that they use appropriate safeguards to protect your data.

VIII. Storing periods for Personal Data

Generally we keep personal data for no longer than is necessary for pursuing or achieving the purposes for which the personal data is processed. However, in most circumstances personal data is processed for more than one purpose, e.g. if the data processing takes place in the context of a purchase we process personal data for the purpose of handling and fulfilling your order, delivering the goods or services, invoicing and payment, and providing customer care afterwards. Yet, as a corporation we also subject to record keeping obligations and have to comply with tax laws and commercial laws that require much longer retention of certain documents and files that may contain personal data.

If we process personal data for the purpose of handling orders and fulfilling contractual obligations we will keep your personal data for as long as you have a customer or business relation with us. Personal data that is included in documents or files that are subject to tax laws will be kept for 10 years (unless statutory provisions or pending lawsuits or tax proceedings require longer retention), personal data that is included in documents or files that are subject to commercial laws will be kept for 6 years (unless statutory provisions or pending lawsuits require longer retention).

If we process personal data for the purpose of understanding your online browsing behaviour we will keep personal data only for as long as necessary to create user statistics and analytics reports that use aggregate data (non-personal data). Specific information as to how long such personal data will be kept is being provided in our [Cookie Policy](#).

If we process personal data for the purpose of communication, marketing, promotion, event and feedback purposes, we will keep the data for as long as we need the data to communicate with you, or for as long as we have a legitimate interest to provide you with business, product and service information, or marketing, event and promotion materials, except where you have objected to the processing of your personal data for such purposes.

If we process personal data for the purpose of compliance with laws and regulations that impose legal obligations on Farnell, we keep personal data for as long as such laws and regulations require.

If we process personal data for the purpose of recruitment and carrying out the application process, we keep personal data for as long as necessary to review and assess the applications, to select applicants, to negotiate and execute an employment contract, and to exercise rights or defend against claims in the context of the applications process. If an application is successful, your personal data – as far as necessary for carrying out the employment contract – will be kept for as long as you are employed with Farnell and after termination of your employment, for as long as necessary to comply with retention

requirements, or for as long as forthcoming or pending lawsuits require longer retention. If your application is not successful we will keep your personal data for up to six months for the purpose of defending us against potential claims and lawsuits.

If your application was not successful, but you have agreed that we keep your personal data on file for future opportunities, we will keep your personal data for up to two years, unless specified otherwise on our careers websites, recruitment platforms or job portals, or in a job advertisement.

IX. Transfers of Personal Data to Third Countries

It may sometimes be necessary to transfer personal data to recipients in other countries. This may be the case as far as certain information that may contain personal data needs to be shared with our parent company Avnet, Inc. in the U.S., or in the context of international cooperation and collaboration with our business partners, or when orders are handled, managed and shipped internationally. If and as far as we make use of the services of processors, we may also transfer your personal data to processors located in other countries.

As far as such data transfers involve recipients in countries outside the European Union or outside the European Economic Area ("Third Countries"), we will ensure that the transfers will be made in compliance with the data protection provisions that restrict the transfer of personal data outside the European Union or the European Economic Area, and which require that appropriate safeguards are implemented to ensure an adequate level of data protection.

Such safeguards could either be an adequacy decision by which the European Union has deemed the country in which the recipient is located to have adequate data protection laws in place, or the execution of EU Standard Contractual Clauses (also known as EU Model Clauses) with the recipient, or the implementation of Binding Corporate Rules ("BCRs") by the recipient, or any other solution permissible at law.

If you have a particular concern about the adequate protection of your personal data when transferred to third countries, you may make an inquiry to the Data Protection Manager at:
DPOCOM@element14.com

X. Security of Personal Data and Protection of Payment Card Details

We have implemented technical and organisational security measures to protect personal data we process against accidental or unlawful manipulation, destruction or loss, alteration, and against unauthorised disclosure or access by third parties. Such security measures include authentication tools, firewalls, monitoring of IT systems and networks, pseudonymisation and encryption of personal data.

The technical and organisational security measures are reviewed and adjusted on a regular basis, taking into account the state of the art of technology, the nature, scope, context and purposes of processing and the risks and probability of occurrence. However, given the dynamic context of security measures, state of the art of technology, vulnerabilities, threats and risks, absolute security cannot be guaranteed.

We may store your payment card details, strictly for the purposes of taking payment for any orders you place with us. We will also store these details to expedite any future purchases you may make with us. We protect any card data we store by revealing only the last four digits of the account number when confirming an order with you. We maintain physical, electronic and procedural controls in connection with the collection, storage and disclosure of any personally identifiable information we store. We take our security obligations very seriously and we would also ask you take sensible measures to ensure that you protect your account details, including ID and password, to prevent them from being used in any unauthorised way. We would recommend that you log out of your account fully and take steps to

delete any browsing history and cookies that may be stored to prevent that information being used by an unauthorised user.

If you have a particular concern about the security of your personal data, you may make an inquiry to the Data Protection Manager at: DPOCOM@element14.com.

XI. Marketing Preferences

As outlined in Section IV. 3. of this Policy, we may have either your consent or a legitimate interest to process your personal details (including name, title, company or organisation you work for, email, telephone, other contact information) to manage your participation in a promotion or event, or to provide you with information about our or our business partners' goods and services, new technological developments, special offers and business opportunities. For these purposes may use your personal details, in accordance with any preferences, if expressed, to send you product and service information and marketing messages by email, post, phone and social media, unless you have asked us not to.

Unless consent is required as a legal basis, which would also require an opt-in, you will always have the opportunity to opt-out of receiving product and service information and marketing messages by simply ticking a box or clicking on a button or link, or by changing your preferences in your account settings, as applicable.

You can of course instruct us in the same way to stop sending you product and service information and marketing messages at any time afterwards. If we are permitted to send marketing information to you, you may opt out at any time (at no cost for email communication other than any carrier data transmission costs). If you no longer want us to contact you for marketing purposes please either [click here](#) to update your preferences or contact us by email at unsubscribe-uk@farnell.com (letting us know what type of marketing you no longer wish to receive) or by telephone on 08447 111113 (charges may apply – please refer to your telecoms provider for further details).

If you instruct us to stop sending you product and service information and marketing messages it might take some time for all our systems and applications to be updated, so you might still get messages from us while we fully process your instruction.

Please note that instructing us to stop sending marketing messages will not stop our other communication with you, such as order confirmations, order updates, shipping notices or payment requests.

XII. Other Websites

Our website may contain links to other websites. Our privacy statement and policy only applies to this website so when you link to other websites you should check the privacy statement on those sites.

From time to time, we may offer you the opportunity to transact using PayPal. Any such transactions will be subject to PayPal's privacy policy which you can view at www.paypal.com under the 'Privacy' link at the foot of their webpage.

XIII. Your Rights over your Personal Data

You have many rights over your personal data and how it is used. These rights are summarised below. In order to assert any of these rights you may contact the Farnell legal entity that is indicated as Controller below in Section XV., or the Data Protection Officer by an Farnell legal entity, if applicable.

1.Right to access your Personal Data

You have the right to request a confirmation as to whether or not we process personal data concerning you.

If we process personal data about you, you have the right to request access to the personal data and to obtain further information regarding the purpose of the processing; the categories of personal data concerned; who else outside Farnell might have received the data, including recipients in Third Countries; any available information what the source of the data was, if you did not provide it directly to us; the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. You may also request a copy of the personal data undergoing processing.

2.Right to rectify your Personal Data

You have a right to rectify (correct) the record of your personal data processed by us, if it is inaccurate or incorrect.

3.Right to erase your Personal Data

You have the right to request erasure (deletion) of your personal data. However, there may be reasons and legal grounds for keeping your personal data despite your request, e.g. if you still have a business relation with us and we need the data to fulfil orders or other contractual obligations, or if record keeping obligations prevent the erasure, or when we handle an ongoing complaint. If we need to continue to process your personal data we will tell you why we need to do this when we respond to your request.

4.Right to object to the processing of your Personal Data

You have the right to object to the processing of your personal data on grounds relating to your particular situation and circumstances. However, there may be reasons and legal grounds for processing your personal data despite your objection. If we refuse your request we will provide you with information explaining why we have refused your request.

As far as we use your personal data for direct marketing purposes, you have the right to object at any time. This includes any profiling of your personal data that is related to direct marketing.

5.Right to restrict the processing of your Personal Data

You have the right to restrict the processing of your personal data. This means that under certain conditions you can limit the way we process and use your personal data. The right to restrict the processing may in particular be exercised if you have issues with the content of the personal data we hold or how it is processed, e.g. if you contest the accuracy of the personal data we hold and we are verifying the accuracy of the data, the processing may be restricted for the time of verification.

6.Right to withdraw Consent to process your Personal Data

Where consent is the legal basis for the processing of your personal data, you have the right to withdraw your consent at any time. However, withdrawal of consent takes typically effect for the future only. Any past processing of personal data that was legitimately based on consent may be subject to other provisions or obligations that require and legitimise further processing of the personal data.

7.Right to portability of your Personal Data

You have the right to request us to move, transfer or copy personal data you have provided to us so that you can use the personal data in a different service or with a different provider. You can request to receive a copy of the personal data in a commonly used and machine-readable format, so you can store it for further personal use. You can also request that we transmit it directly to another organisation.

However, the right to data portability may be subject to limitations due to the technical feasibility of a transmission. The right to data portability does not create an obligation for us to adopt or maintain processing systems which are technically compatible with those of other organisations.

8.Right to lodge a complaint with the Data Protection Supervisory Authority

You have the right to lodge a complaint with the relevant Data Protection Supervisory Authority if you believe that we have not handled your personal data correctly and lawfully or if you believe that we have not dealt appropriately with your requests.

The relevant Data Protection Supervisory Authority where the complaint should be made is the one that is competent for your place of residence or your state or to the supervisory authority which is competent for us. This is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom

When you have lodged a complaint, the Data Protection Supervisory Authority will inform you of the progress and outcome of the complaint.

XIV. How to contact us on Data Protection

If you have any questions or concerns about this Data Protection Policy or about the protection of your personal data, please feel free to contact our Data Protection Team at: DPOCOM@element14.com Some of Farnell's legal entities have appointed a Data Protection Officer. If applicable, you may also contact the Data Protection Officer directly at the contact details specified by the respective Farnell's legal entities.

XV. Data Controller and Responsibility

Unless indicated otherwise, the Farnell company operating this website, is the controller of your personal data. It determines the purposes and means for processing your personal data and is responsible for compliance with applicable data protection laws and regulations and the requirements of this Policy.

XVI. Amendments to this Policy

We reserve the right to amend this Policy at any time. This Policy can be amended under the defined procedure for amending policies and notifying amendments.

Appendix A: Glossary and Definitions

Accountability Principle means that controllers will be responsible for, and be able to demonstrate compliance with the GDPR which requires the controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures where necessary.

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.

Data Protection Policy means this EMEA Data Protection Policy.

Data Processing Agreement means an agreement that forms part of the master agreement between a controller and a processor to reflect the parties' agreement with regard to the processing of personal data, in accordance with the requirements of Data Protection Laws.

Data Protection Impact Assessment means the process to assess the particular likelihood and severity of the high risk to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing and the sources of the risk; an impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with the GDPR.

Data subject means an identified or identifiable natural person ; 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.

GDPR means the General Data Protection Regulation, being Regulation **(EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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.**

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.

Personal data means any information relating to (i) an identified or identifiable natural person and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations).

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.

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.

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

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.

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.

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

Special Categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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.