AURORA

ENERGY RESEARCH

Privacy Strategy, Principles & Policy

Official Publish Date: November 2020

AURORA ENERGY RESEARCH

Contents

1 About This Document

1.1 Introduction

This document contains the Aurora Energy Research Limited ("Aurora") Privacy Strategy, Privacy Principles and Privacy Policy. It governs and supports all of the business activities of Aurora in our processing of personal information.

The Privacy Strategy contains the privacy mission, vision and objectives consistent with Aurora's business and corporate values.

The Privacy Principles are the basic rules that guide Aurora's efforts as they relate to privacy and the handling and protection of personal information. These Privacy Principles are widely available, published for all internal and external audiences, including clients, associates, employees, clients and vendors.

The Privacy Policy is a document that expounds upon the Privacy Principles and provides high-level guidance on actions Aurora is to take relating to personal privacy. Compliance with the Privacy Policy and Principles is mandatory for all Aurora personnel and business entities (as described below) per our corporate implementation schedule. The Privacy Policy includes common questions concerning Aurora's privacy program, its privacy practices and areas of general privacy concern. The Privacy Policy may be provided upon request under a Non-disclosure Agreement to clients or other 3rd parties who have a need to understand our commitment to privacy.

1.2 Aurora's Privacy Framework

The following Privacy Management Processes together make up an operational privacy framework that is an expression of Aurora's privacy program:

1. Maintain Governance Structure:
    a. Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures.
    b. Maintain and review reporting pathways to ensure appropriate continuing oversight.
    c. Regularly consider and update metrics by which discharge of responsibilities in this area will be monitored and assessed.
2. Maintain Personal Data Inventory:
    a. Maintain an inventory of the location of key personal data storage or personal data flows with defined classes of personal data.
    b. Ensure, through a programme of review and testing, that this inventory is accurate, up to date, and capable of being functionally interrogated as required.
3. Maintain Data Privacy Policy:
    a. Maintain a data privacy policy that meets legal requirements and addresses operational risk.
    b. Operate a programme of regular review and assessment against changes to business operations; evolving standards and the wider regulatory/ compliance landscape.
4. Embed Data Privacy into Operations:

   a. Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives.
5. Maintain Training and Awareness Program:
   a. Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks.
   b. Review reporting of incidents and near misses to assess the effectiveness of this program and to identify topics which require further/additional emphasis in future.
6. Manage Information Security Risk:
   a. Maintain an information security program based on legal requirements and ongoing risk assessments.
   b. Regularly assess the appropriateness of the technical and organizational safeguards in place within the business, having regard to the risk posed by a potential breach of the data in question, available resources and the state of the art.
7. Manage Third-Party Risk:
   a. Maintain contracts and agreements with third parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance.
8. Maintain Notices:
   a. Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance.
9. Maintain Procedures for the Exercise of Data Subject Rights, Enquiries and Complaints:
   a. Maintain effective procedures for interactions with individuals about their personal data.
   b. Maintain systems which are capable of giving timely and substantive effect to the data subject rights that employees, customers or others might exercise.
10. Monitor for New Operational Practices:
   a. Monitor organisational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles.
11. Maintain Data Privacy Breach Management Program:
   a. Maintain an effective data privacy incident and breach management program.
12. Monitor Data Handling Practices:
   a. Verify operational practices comply with the data privacy policy and operational policies and procedures.
13. Track External Criteria:
   a. Track new compliance requirements, expectations, and best practices.

1.3 Scope and Application

1.3.1 Aurora Business Entities

This document will govern all business entities of Aurora, including Aurora Energy Research GmbH. This document will govern Aurora joint ventures with other organizations if specifically identified in this section. Throughout this document, "Aurora" should be understood as encompassing ultimately all of these entities in all locations.

1.3.2 Business Processes

This document will govern all business activities that involve the processing of Personal Information undertaken by Aurora and any person working under Aurora's direction or control. This document is designed to help manage the risks associated with these business activities.

1.3.3 Data Subjects

A "Data Subject" is any individual about whom Aurora processes Personal Information ("PI"). We process PI from (or pertaining to) various groups of persons including clients, potential clients, attendees at Aurora events, journalists, suppliers, other business partners as well as employees and potential employees. We also process PI about persons who have contact with us through our relationships with our clients, suppliers, vendors, sub-contractors, and other business partners and third parties.

Aurora will most often be a data controller, which is the person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of PI. For example, the data controller determines what PI is to be collected and how the information is to be collected, stored, used, shared, and destroyed. Aurora may also sometimes be a data processor, which is a natural or legal person, public authority, agency or any other body that processes PI on behalf of a data controller.

Aurora is typically a data controller for personal information it collects from clients, subscribers, employees, attendees at Aurora events, journalists, suppliers, other business partners as well as potential clients interested in Aurora services.

Note that in the unlikely event that Aurora considers that it is processing PI as a data processor on behalf of a third party controller, there must be a formal written data processing agreement in place with the data controller of that PI, and Aurora must only process in accordance with the provisions of that agreement.

1.3.4 Data Classifications (Categories of Personal Information)

Some PI is handled differently depending on the sensitivity of the data:

- Personal Information ("PI")
    - Any and all information that relates to an identifiable person. This includes addresses, telephone numbers and emergency contact details.
    - Information concerning legal entities for information processed in and exported from certain other countries as required by the specific national laws.
    - There are two specific sub-categories of PI which described separately in Aurora's policies and privacy framework:
- Sensitive Personal Information
    - Sensitive Personal Information is a higher risk subset of PI that consists of:
- Data elements that are specially protected by law, including details of nationality or ethnicity; health information; information about political affiliation or sexual identity;
- Personal financial information including, for example, employees' sort codes and account numbers or customer credit card details; and
- Government-Issued ID details such as passports, visas and National Insurance numbers
- Contact Information

- Contact information is a lower risk subset of personal information that contains only business contact information (such as the information published on a business card). Contact information may include name, title, company affiliation, mailing address, phone and facsimile numbers, SMS text contact information, email address, and preferred contact preferences (method and time of day).

1.4 Maintenance and Administration

1.4.1 Business Changes

Business changes that result in a significant addition or change to the nature or handling of personal information may necessitate revisions to this document and other documentation within our privacy framework. Such changes will be developed and approved by Head of Operations.

1.4.2 Regulatory Changes

Regulatory changes may necessitate revisions to this document and other documentation within our privacy framework. Such changes will be developed and approved by Aurora's Legal Counsel (Meng He).

1.4.3 Ownership and Responsibility

Ownership and responsibility for this document, and its component parts, rests with Aurora's Head of Operations and the Aurora Legal Counsel. Questions and requests to update (e.g. per business or regulatory changes) should be directed to Head of Operations.

1.5 Privacy

"Privacy" (of which "data protection" is an important part) can best be defined as the assurance that PI is being processed in an appropriate, legally-compliant and secure manner. Each individual's privacy interests extend to Collection, Storage, Use, Sharing, and Destruction of PI. What is considered "appropriate" varies among countries and cultures, and the legal requirements that apply vary as well. For example, in the United States, this translates into a regime where data processing is appropriate as long as persons are not harmed by the data processing. In Europe and other countries, however, privacy is considered a fundamental human right, and data processing cannot occur without meeting strict requirements even if no one could be harmed. The concept of privacy therefore has broad implications for how Aurora manages PI for its business processes.

1.6 Regulatory Requirements

This document is built on a baseline established with reference to a specific set of regulations, business practices and obligations identified by Aurora as most critical to its worldwide operations. It will also include many of the local regulatory or contractual requirements, when different from the baseline. If you have a question about compliance with privacy and other laws in a particular location or relevant to a specific business market or business line, please contact the Head of Operations.

Please note that it is the responsibility of each Aurora business unit to confirm its compliance with all applicable local laws.

1.7 Terminology

The Appendix to this document contains a glossary, which establishes a vocabulary for Aurora to use to communicate about privacy both internally and externally. For the meaning of other terms found in the principles, policy and guidelines, and throughout the Aurora Privacy Framework, please refer to the glossary.

2 Privacy Strategy

Aurora's privacy mission, vision and objectives are to address privacy from a number of perspectives. These are identified by basis:

2.1 Legal Basis

- Aurora and its affiliates may be exposed to government penalties and private action for failure to comply with privacy laws in the United Kingdom and the European Union.

2.2 Commercial and Client Basis

- Aurora clients have asked about our compliance status during the tender process and our client contracts include privacy compliance language;
- We are approached by new and existing clients on a regular basis to start new projects or continue or extend;
- Client events are crucial to business development and discussion of global energy issues;
- Aurora's new business models require regional and often global flows of information to deliver the services;
- Data centre consolidations and global systems depend upon a consistent flow of PI;
- Auditing requirements

2.3 Value Basis

- Our values stipulate that we respect our employees, colleagues and clients and are committed to providing services in an ethical manner

2.4 Public Relations Basis

- Government, civil or client actions taken against Aurora could diminish Aurora's image in the marketplace

Given the various bases above, the strategy of Aurora is to develop data privacy goals and objectives consistent with legal requirements, commercial obligations and Aurora's business values, while respecting the privacy of the individual personal information Aurora collects. Aurora also strives, at the same time, to create a common basis for Information Management upon which Aurora can more comprehensively serve national and international clients and clients and more consistently build global systems and create consolidated data centres. This is to be achieved by:

1. Consistent Practices: Privacy practices being more consistently applied and better integrated into Aurora's business processes;
2. Defined Responsibilities: Responsibilities for privacy being better defined;
3. Awareness and Training: Privacy awareness being significantly improved;
4. Adequacy of Data Transfer: Putting mechanisms in place to support adequacy & meet Aurora's privacy requirements & our datacentre consolidation & global system schedules
5. Security Improvements: Security being improved where issues are identified.

The focus of the overall program is based upon a rationalized and risk based approach to data privacy, ensuring that we have adopted the most important laws and best practices from the industry as a whole across our companies and countries.

3 Privacy Reporting

Aurora has established a privacy organisation that includes a Privacy Officer (Aurora's Head of Operations).

The Privacy Officer approves the privacy strategy, policy(s) and overall program; represents privacy matters to the executive committee and the board of directors.

The Privacy Officer directs strategy; maintains the global principles, policy, standards and tools; creates global solutions; oversees the Office of Privacy; facilitates implementation; and coordinates the response to major incidents.

The Privacy Officer approves the privacy program; advises, approves and supports local implementations; addresses constituent interests and concerns; and shares ideas and tools.

4 Privacy Principles

At Aurora, privacy matters. It is an inherent part of our values, which stipulate that we respect our employees, colleagues, clients and business partners and are committed to providing services in an ethical manner. That's why Aurora has established the following set of privacy principles.

Aurora's privacy principles are based on internationally recognised fair information practices and principles and are in the spirit of Aurora's ethic. The following principles are embodied in Aurora's Privacy Policy. Together, the principles and policy express and support Aurora's privacy commitment to our clients, our workers and all persons with whom we have business interaction.

4.1 Aurora's Privacy Principles

Aurora has long recognized the importance of maintaining the privacy of personal and sensitive information of our employees, clients, vendors and partners. The nature of our business requires us to collect and handle such information, and we have a responsibility to protect this information for as long as it is in our possession. At Aurora, respecting our employees, colleagues and clients is a part of our core values, along with being committed to providing services in an ethical manner.

To support these obligations, Aurora has created a set of global data privacy principles, which guide our efforts as they relate to privacy and the handling and protection of PI and (particularly) sensitive personal information.

Aurora's Data Privacy Principles:

We respect your privacy when:

- We offer privacy notices that explain how and why we handle personal information.
- We respect your choices about our collection, use and sharing of information.
- We collect, use and retain only personal information that is relevant and useful to our business interactions.
- We use reasonable efforts to keep personal information accurate and up-to-date.
- We use information security safeguards to protect personal information.
- We limit access to and disclosure of personal information.
- We retain personal information as needed to fill our legal and business obligations.
- We provide an opportunity for you to ask questions and register complaints about privacy and exercise rights such as the right to access your data or to have your data erased.

5 Privacy Policy

5.1 Introduction

Aurora recognizes and supports the privacy interests of all persons, and we respect these interests when we collect and process PI. We have developed and adopted a set of Privacy Principles that define our privacy values. We have also developed and adopted this Privacy Policy to describe and guide our processing of PI. This Policy is accompanied by some frequently asked questions to illustrate and clarify the Policy.

As a preliminary matter, it is the responsibility of all employees to assist in the protection of PI by acting in accordance with this Policy. Each employee is also responsible for helping to ensure that the PI we hold is accurate and up-to-date.

In addition to the restrictions and obligations of this Policy, we always comply with the letter and spirit of applicable national laws that protect the privacy of PI. This Policy also applies in nations where we operate, that do not have privacy or information protection laws.

5.2 Clients and Aurora

At Aurora, information about our clients is an essential element of the superior service that makes our business successful.

5.3 Our Privacy Commitment

At Aurora, privacy matters. We respect the privacy of our clients, suppliers and other individuals with whom Aurora has business interactions. And we respect the privacy of our staff – our most valuable asset. That's our privacy commitment.

5.4 Scope

This Policy applies to all PI that is collected, maintained, or used by any division, business unit or affiliate of Aurora. This includes its principal operating units: Research and Publications, Consulting Projects, Commercial and Operations. The terms of this Policy are also intended to apply to agents and contractors that handle and process personal information on behalf of Aurora.

The Policy applies to all PI collected by Aurora, for all the services we provide externally and to our internal processes, including:

- Sales and marketing processes including interaction processes with clients, potential clients and other business partners, including logins to the EOS platform, written summaries of client telephone conversations in the Salesforce platform;
- Service and content delivery processes;
- Data cleansing;
- Data transport;
- Recruitment, applications for visas, payment of employees, performance management and workplace management;

This policy will also apply to information concerning legal entities for information processed in and exported from certain other countries as required by the specific national laws.

This Policy applies to personal information in any format. For example, the Policy applies to computerised records and electronic information as well as paper-based files.

This Policy is global, applying to all Aurora locations. This policy is the imperative basis for using PI and can only be replaced by stricter national regulations.

This Policy applies primarily to PI that we collect and use for our own business purposes. In some cases, Aurora processes PI that belongs to other companies, such as our clients or other business partners. In these cases, Aurora shall protect the PI, comply with all laws that regulate the information, and use information only as authorised by the data owner. Other inconsistent provisions of this Policy will not be applicable to PI that we hold as a processor for these other companies.

5.5 The Information We Collect and Use

We collect and use the PI to support and further our businesses. We will collect PI directly from individuals wherever practical, and always in accordance with the law. The types of information and the purposes for which we collect PI may include:

For Employees

Aurora collects and uses PI as needed for human resources and employment processes from current and prospective employees, associates and independent contractors. Aurora collects this information only in a reasonable and lawful manner.

Aurora uses such PI only for relevant, appropriate, and customary purposes, such as: (1) recruitment and placement; (2) administration of compensation and benefit programs; (3) performance management and training; (4) advancement planning; (5) workforce and risk management, (6) workplace management, (7) government reporting and (8) other legal and expected business-related purposes.

- For example, Aurora receives PI in connection with recruiting. This information may be submitted to us electronically, on a form, in correspondence, or in conversation. Aurora may also collect information from job posting boards. The PI may include the applicant's name, contact details and preferences, education, skills, references, work experience, job preferences and salary expectations. This information is used to assess the person's suitability for a position, and to negotiate and make offers of employment or assignment.
- We may also receive PI about individuals from third parties through enquiries we make to verify details provided to us in an application, such as references, credit or background checks, and certifications.
- We will also need to receive the PI needed to establish and maintain an employment with the individual, such as work history and assignment details, salary, performance information, work and residency permits, time and expense reporting information, and bank account and other information needed for personnel management.

For Clients

Although our clients are companies, Aurora collects the PI (such as email addresses and phone numbers) of some of the individuals within the client organizations we work with. This contact information and other personal details are used to provide support and improve the services we provide.

Aurora collects and uses PI as needed to deliver its products and services and manage its business. Aurora collects this information only in a reasonable and lawful manner.

Aurora uses such PI only for relevant, appropriate, and customary purposes, such as: (1) selling products and services; (2) delivering products and services; (3) providing advice and answering client requests; (4) inviting individuals to events and conferences; (5) processing transactions; (6) administrating accounts; (7) marketing; (8) product and service management and analysis and (9) government reporting, other legal and expected business-related purposes.

For example, we may obtain client PI;

- when potential clients approach us via email, via phone, or via our website,
- when client or potential clients join our webinars,
- when we meet clients and potential clients at conferences or other events,
- when we meet client members in client meetings,
- when clients access our data platform and download reports or other data,
- when we collect publicly available information from the internet and similar sources

We also sometimes collect PI about our client's clients. Where we provide our clients with products and services for their clients, we collect much of the PI identified above.

For Vendors, Suppliers and Sub-Contractors

Aurora collects PI about individuals who are employed by our suppliers and vendors. This contact information and other personal details are used to administer existing and future business arrangements

Others

Additional PI may be collected, used and disclosed for the purposes for which it was collected and for legal compliance purposes, including regulatory reporting, investigation of allegations of wrongdoing, and the management and defense of legal claims and actions, and compliance with subpoenas, court orders and other legal obligations. For example, we may collect information about individuals that visit our facilities.

5.6 Privacy Notices

Where possible, we inform individuals about our privacy Principles and our processing of their information. We also make this information available upon request. In particular, our privacy notices contain:

- the type of information we collect;
- the purposes for which we collect PI;
- the type of parties to whom we disclose PI;
- the privacy and information safeguards we employ;
- how to access and correct PI (if appropriate), and;
- what choices the individual has with respect to the collection, use or disclosure of the information.

We also offer transparency with regard to international information transfers. Our privacy notices include information about the safeguards that Aurora has put into place to help ensure an adequate level of protection for the transferred information.

5.7 Choices and Accommodation

Aurora provides individuals with a reasonable opportunity to object to the collection, use, and disclosure of their PI. We also seek to make reasonable accommodations when an individual has concerns about our processing of PI.

In addition, where consent of an individual for the collection, use, or disclosure of personal information is required by law, contract or agreement, we request such consent and respect the individual's choice in such matters. For example, as discussed below, in some countries, consent is required before sensitive information [SPI] about individuals can be processed or transferred. In these countries, we must receive consent prior to the processing or transfer of the sensitive information.

5.8 Sensitive Information

There are certain types of personal information that we consider to be particularly sensitive and for which we provide additional and appropriate privacy protection and confidentiality. We will only collect and use this sensitive information where there is a legal basis, or where we have obtained the individual's consent or where there are compelling business reasons if legally permitted.

"Sensitive Information" held by Aurora is personal information relating to an individual's:

- Race or ethnic origin;
- Physical or mental health or conditions;
- Sexuality and gender;
- Political affiliations or trade union membership;

- Criminal records (or allegations of crimes);
- Financial information (such as bank account number), and;
- Government issued identification numbers (such as National Insurance number, Passport details, Visa details or drivers license)

We collect and use sensitive information for the following types of purposes:

- To verify an individual's identity and assess suitability for a position or task. In certain cases, the job opportunity may warrant additional security checks including information on previous offences and criminal records
- As required by law. For example, to process payroll, entitlements, claims, benefits and deductions, and to help us comply with our legal and regulatory obligations, such as accounting and tax reporting and health and safety management
- For internal compliance and security programs, such as workplace safety, access badges, diversity monitoring and anti-discrimination programs

5.9 Accuracy of Information

We employ reasonable means to keep PI reasonably accurate, complete, and up-to-date, as needed for the purposes for which it was collected

5.10 Information Disclosure

Internal Disclosure

In general, PI may be shared within Aurora, where legally permitted for reasonable and appropriate corporate purposes. However, even within Aurora, we restrict access to PI to those employees, agents, or contractors who need access to carry out their assigned functions.

External Disclosure

Disclosure of PI beyond the employees, agents, or contractors of Aurora, may be made only pursuant to an agreement, business necessity, as permitted or required by law or legal process, or with the consent of the individual. The following examples illustrate some of the reasons that PI is disclosed to third parties about:

Employees

We may disclose PI about workers and employees to a range of third parties who provide our employees with services, such as pensions management. We may also disclose PI to government departments where necessary in order to comply with residency requirements or income tax reporting.

All Individuals

PI may always be disclosed in connection with legal compliance initiatives, in response to a government request for information or as part of the due diligence, negotiation and completion of a sale or transfer of all or part of Aurora.

5.11 The Location of Personal Information

PI may be stored and processed in and transferred between a local Aurora branch, at Aurora's UK office, at the locations of our service providers and clients, at one or more of our international data centres and in the cloud via our service providers.

5.12 Protecting Personal Information

To help protect the confidentiality of PI, Aurora employs security safeguards appropriate to the sensitivity of the information. These safeguards include reasonable administrative, technical and physical measures to protect the confidentiality and security of PI against anticipated threats and unauthorized access to the PI.

We expect the same commitment from our agents and suppliers who receive personal information from or on behalf of us in the course of their relationship with our organization.

5.13 Access and Correction

We shall generally provide individuals with an opportunity to examine their own PI, confirm the accuracy and completeness of their PI, and have that PI updated, if appropriate.

The ability of an individual to access their PI is not unlimited, however. An individual's ability to access PI may be limited, for example, where (a) the burden or expense of providing access would be unreasonable or disproportionate to the risks to the individual's privacy, (b) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or (c) providing access would compromise the privacy of another person.

5.14 Marketing

We use contact information of our clients, clients and other business partners for marketing purposes. We may also periodically communicate with workers and employees about services that we offer. In every case, we comply with all laws applicable to the marketing communications being transmitted.

We provide our clients with the relevant choices for sharing or not PI within our affiliates, business partners and third parties.

6 Annex A – Key Definitions

Data Subject	"Data subject" means any natural person whose information is being processed by Aurora as a controller or a processor; *[source GDPR]*
Personal Data	"Personal Data" is 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. *[source GDPR]*
Special Category Data	"Special Category Personal Data" is any information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, genetic or biometric data, criminal offences, or related proceedings—any use of special category personal data should be strictly controlled in accordance with this policy.*[source GDPR]*
Controller	"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. *[source GDPR]*
Processor	"Processor" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller. *[source GDPR]*
Recipient	"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. *[source GDPR]*
Processing	"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. *[source GDPR]*
Profiling	"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. *[source GDPR]*
Pseudonymisation	"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. *[source GDPR]*
Filing System	"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. *[source GDPR]*
Consent	"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. *[source GDPR]*
Personal Data Breach	"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. *[source GDPR]*