Altran Data Protection Policy

Reference	Classification	Owner
Altran Data Protection Policy	ALTRAN Official	Group DPO

Version	Last update	Comment
V2.0	April 22nd, 2020	improvements on v1

Content

1.Introduction

1.1 Purpose of the document

Altran provides its clients with engineering R&D solutions and, as a global leader whose activities stretch out worldwide, undertakes to ensure personal data protection under its responsibility.

With the reinforcement of data protection regulations, Altran wants to reinsure its clients, employees and business partners that their safety and well-being are its chief concern and so it is entirely committed to the protection and respect of their personal data.

We used the General Data Protection Regulation (GDPR) as a guideline when we designed this policy. This document is of course for our clients, employees and business partners but also for any competent authority or person interested in Altran data protection policy.

Besides, we exceed GDPR provisions every time we think it is necessary or expected by our clients or partners. Furthermore, this policy will continuously take into account any other relevant requirement set by data privacy rules and regulations.

1.2 Scope

Altran data protection policy applies to all processing of personal data, including initial collection, storage, use, forwarding within the company and transfer to third parties. It fully regulates all aspects of data protection law that may be relevant within the context of data processing. It applies to all types of personal data, in particular data related to present or past employees, customers, suppliers and other business partners.

1.3 Update of the policy

Altran Data Protection Policy keeps developing as data protection stakes never stop changing in a technologic and legal environment that evolves fast. Thus, the Altran privacy team reviews our policy at least once a year to keep it up to date.

1.4 Definitions

Personal data: any information relating to an identifiable person or identified person (data subject)

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

GDPR: the European Union legal frame for processing of personal data, it was adopted in April 14th 2016 and came into force in May 25th 2018.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

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

Data protection officer (DPO): a person Altran specifically names to monitor internal compliance with the GDPR. The DPO informs and advises Altran and its employees about their rights and obligations. The Data Protection Leader (DPL) is his or her relay for a specific geographical entity (GEO) or Business Unit (BU).

Record of processing activities: a register of all Altran personal data processing device with information about the processing and the processed data.

2. Context of personal data processing

2.1 Altran internal activity

This activity concerns all personal data collected and processed by Altran or its sub-contractors in the context of its own activities, like any other company. It involves processing the personal data of its employees for the following types of activities (non-exhaustive list):

- Human resources management
- Management of financial and accounting operations
- Management of sites
- Management of IT resources
- Management of communication
- and in general, any activity enabling us to ensure the realization of our legitimate interests or to comply with our legal or regulatory obligations

In the context of these activities, Altran is, in principle, considered by the regulations to be a data controller.

2.2 Altran activities for third parties

This activity concerns all personal data processed by Altran or its subcontractors in the context of relations with our:

- clients as a subcontractor
- suppliers, in their capacity as Data Processors
- partners on research projects, partnerships or corporate projects, in their capacity as Data Controller or Joint Data Controller

All activities giving rise to regular and structured processing of personal data within these areas are brought to the attention of the local Data Protection Officer, and/or the Data Protection Leader, who include them in Altran personal data processing register.

3. Altran Compliance Governance

Altran compliance program with the regulations governing the processing of personal data is carried out at Group and Geos levels. The Executive committee of Altran ultimately has responsibility for ensuring that the Company complies with its obligations in relation to privacy and the processing of personal data

At the Group level, an Executive Committee made up of personalities from the Altran Group top management has been set up and meets every month to monitor the Group's compliance in this area. This committee has appointed a Data Protection Officer (DPO) for the Group (available at dpo.group@altran.com) who has been declared to the French data protection authority, the CNIL.

At the Geo/BU level Data Protection Officers (DPO) and Data Protection Leaders (DPL) have been appointed to locally relay the action of the Group DPO. They are also responsible for ensuring the compliance of their reporting entity with locally applicable legislation on the processing of personal data.

Group DPO, DPOs and DPLs meet every month to:

- share information
- synchronize on implementation activities (policies, procedures - monitor compliance KPIs.

4.Measures and commitments

4.1 Guiding principles for the protection of personal data

Altran processes personal data in accordance with the principles of personal data protection the GDPR expresses:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- confidentiality and integrity
- accountability
- privacy by design and by default and data privacy impact assessment

Altran creates and maintains a set of documentation to demonstrate compliance with the above principles in the context of its various activities.

4.2 Lawfulness, fairness and transparency of personal data processing activities

To ensure its processing of data is lawful, fair and transparent, Altran maintains record of processing activities. The record is reviewed at least annually. Data subjects have the right to access their personal data and any such requests made to Altran is dealt with in a timely manner.

All data processed by Altran are done on one of the following lawful bases: consent, contract, legal obligation, vital interests or legitimate interests. Altran notes the appropriate lawful basis in the record of processing activities. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent is kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent is clearly available and systems are in place to ensure such revocation is reflected accurately in Altran systems.

Altran takes appropriate measures to provide all relevant information when personal data are collected from the data subject either directly or indirectly. These measures may include, but are not limited to, the following:

- The publication of information on the intranet and the various Altran websites;
- Posting relevant information in places accessible to the data subjects on the various Altran websites;
- The insertion of legal notices, clauses and contractual annexes in the various legal documents governing Altran activities, both within the framework of its internal activities and in the context of its relations with third parties.

4.3 Purpose Limitation

Altran processes personal data for specified, explicit and lawful purposes and in a manner consistent with those purposes (and personal data will not be processed in any manner which is incompatible with the specified, explicit and lawful purposes for which it was obtained).

Unless the applicable law provides otherwise, informed consent is sought from a relevant data subject through appropriate disclosure of information at time of collection or processing of personal data.

4.4 Data Minimization

Altran ensures that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Company will ensure that when personal data is no longer required for specified purposes, it will be deleted or anonymized in accordance with our record retention policies.

4.5 Accuracy

Altran takes reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps are put in place to ensure that personal data are kept up to date.

4.6 Storage limitation

To ensure that personal data is kept for no longer than necessary, Altran puts in place a data retention policy for each area in which personal data is processed and review this process annually. This policy considers what data should/must be retained, for how long, and why.

4.7 Confidentiality and integrity

Altran ensures that personal data is stored securely using modern software that is kept-up-to-date. Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information. When personal data is deleted this is done safely such that the data are irrecoverable. Appropriate back-up and disaster recovery solutions are in place. Personal data is not disclosed to an unauthorised third party without a clear 'need to know' reason being identified prior to disclosure, and in accordance with the information provided to the data subject

All internal and external employees are subject to a duty of data secrecy. Employees who joined Altran after the entry into force of the GDPR have already undertaken to comply with this duty of data secrecy by signing the employment contract.

Adequate security measures (but are not limited to) ensure:

- Prevention of unauthorized and unauthenticated persons from gaining access to personal data processing systems in which personal data are processed by implementation of appropriate technical measures
- Confidentiality, integrity of personal data in motion and at rest
- Physical security of organization assets containing personal data
- Personal data are not kept longer than stipulated in accordance with local data retention processes, including by requiring that personal data transferred to third persons be returned or securely destroyed. Creating copies of personal data must be restricted to legitimate business purposes, they must be disposed securely after use or retention period

4.8 Removing Personal Data from Company Locations or systems (Including Home Working)

Personal data may not be removed from Altran locations without appropriate measures having been implemented to ensure the continued security of the personal data and its protection from unauthorised damage or destruction.

Where personal data are stored on or processed by means of portable or removable media (for example, laptops, tablets or mobile phones), or where Company personnel are processing personal data while working from home or away from Company locations, then appropriate encryption or other technology should be used to ensure that personal data remains secure.

The Company's policies with regard to home working and the use by Company personnel of their own devices should be complied with at all times.

4.9 Rights of persons concerned by the processing of personal data

Altran is deeply committed to respect the rights the GDPR gives to data subjects and ease the way to enforce them. The existence of the privacy team (DPO and DPLs) and its large geographic scope make possible to handle on due time data subjects' requests from all around the world. The main rights in question are the following right:

- of information
- of access
- to rectification
- to erasure
- to restriction to processing
- to data portability
- to object
- to not be subject to a decision based solely on automated processing, including profiling
- to withdraw consent
- to lodge a complaint with a relevant supervisory data protection authority or court.

4.10 Security of personal data processing

Altran ensures the security of personal data under its responsibility by implementing data protection reinforced by the use of organizational, physical and logical security measures.

4.10.1 Criticality of personal data and processing

Every processing of personal data carries a risk regarding data protection. This risk is assessed according the nature of the processed data and the purpose of the processing.

Some data are considered as low-risk like identification data and some others as high-risk, sensitive data for example. Likewise, we consider some processings as low-risk because of their purpose, for instance recruitment and personnel management, and others as high risk still because of what they aim to, for example data transfers outside the European Economic Area (EEA).

Once we have assessed the sensitivity of processed data and the risk the processing carries in itself , we can set the processing level of data protection impact

According to the results of the risk assessment, Altran decides whether it is necessary or not to carry out a data protection impact analysis.

4.10.2 Organizational Measures

The risk principle described above allows Altran to treat the subject of personal data protection "by default". The measures taken in relation to the criticality of the processing of personal data differ depending on whether one is considering a purely internal Altran activity or an activity on client's behalf:

- Altran internal activities: each Altran business process owner must define the level of criticality of the data and processing carried out in order to provide the necessary security measures with regard to the risks identified;
- Altran activities for third parties: each project set up by Altran for a Client must define the level of criticality of the data and processing in order to provide the necessary security measures in relation to the risks identified.

4.10.3 Prevention of new non-complying systems

The Company's Information Technology Department shall, under the guidance of the Data Protection Office and shall establish and maintain suitable procedures for the assessment of any new technology/systems before they are deployed to ensure that they meet the requirements of this Policy and comply with all relevant applicable privacy laws.

4.10.4 Operational measures (physical and logical)

Each business process owner is responsible for defining the security measures to be implemented and enforced with regard to the various criticalities and risks, depending on the context.

4.10.5 Breach management

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, Altran promptly assesses the risk to data subjects' rights and if appropriate report this breach to the Data Subjects and/or CNIL as the case may require.

4.11 Privacy by Design & Data Protection Impact Assessments (DPIAs)

Altran assesses privacy by design measures that can be implemented on all programs/systems/processes that process personal data by taking into account the following:

(a) the state of the art and cost of implementation

(b) the nature, scope, context and purposes of processing along with the risks and impacts associated

Altran conducts a DPIA (and discuss the findings with the DPO) when implementing major system or business change programs involving the processing of personal data for automated profiling, analysis of sensitive information, and systematic monitoring

4.12 Data transfers outside the EEA

Altran is a group operating worldwide and therefore some personal data it processes go beyond the European Economic Area boundaries where GDPR applies. It does not rise any concern if the data are sent in a State whose data protection law is ruled as providing an adequate level of protection by the European Commission[1] or benefiting from a special legal mechanism for data transfers[2]. Otherwise, Altran has designed a data protection agreement. The latter ensures a legal frame as protective as GDPR to all Altran data processing wherever they take place and whoever's personal data are processed.

4.13 Enforcement of Privacy Violations by Company Personnel

The DPO function is responsible for working with Company personnel and the Company's advisors to ensure compliance with applicable laws, regulations and obligations. The results of each internal investigation following a violation, including any disciplinary action recommended or taken, will be reported to the Data Protection Office. Where the Company believes that the conduct may constitute a violation of any applicable law, rule or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

4.14 Training

The Company will ensure that all employees receive a copy of this Policy as part of their new hire orientation information and will, as part of their on-boarding with the Company, be given basic training on privacy and security related issues.

4.15 Direct Marketing

The right to object to direct marketing by Altran to data subjects must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honored. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

---

[1] Andorra, Argentina, Faroe Islands, Guernsey, Israel, Japan, Jersey, Isle of Man, New Zealand, Switzerland et Uruguay

[2] « Privacy Shield » in the United-States and the Personal Information Protection and Electronic Documents Act in Canada

4.16 Complaints

Personnel with enquiries or complaints about the processing of their personal data may contact their local human resources manager (in case of company personnel), or any member of the Data Protection Office (available at dpo.group@altran.com)

The Data Protection Office will investigate on all such enquiries or complaints. Issues which cannot be resolved by the Data Protection Office shall be dealt with in accordance with established grievance procedures or other non-judicial procedure as established by applicable contracts agreements, or statutory provisions.

4.17 Principle of responsibility for regulatory compliance

Altran has created and kept a corpus of documents to demonstrate compliance with its legal and regulatory obligations in terms of personal data protection. This documentation package includes, but is not limited to, the following:

- The register of personal data processing, listing all of Altran activities involving data processing activities and tracing for each of them the main stages of the life cycle of personal data in each processing operation;
- Personal Data Protection Impact Analyses, which make it possible to assess the criticality of each project that may involve a significant risk to the rights and freedoms of data subjects and to determine the measures that could be taken to prevent the main risks for data subjects (cf. 2.4.1).

Altran specific data protection policies :

- Information security policy
- Data retention policy
- Data governance policy.