Personal Data Protection Policy

data:respons
part of AKKODIS

DATA RESPONS - PERSONAL DATA PROTECTION POLICY

Last update: 16/02/2022

Introduction

Data Respons is committed to comply with the requirements of the EU General Data Protection Regulation 2016/ 679 ("GDPR") in relation to how it holds and/or uses personal data.

Data Respons entities process many types of personal data for business and HR purposes concerning job applicants, employees, former employees, workers and contractors, partners, suppliers and customers (aka. "Data Subjects"). The Data Respons entity with whom you have signed a commercial or contractual relationship is primarily responsible for processing your personal data, thereby acting as "controller" as defined by the EU GDPR, as it decides why and how your personal date are being processed within the Group.

Data Respons is fully aware of its obligations under the GDPR to process personal data lawfully and to ensure that the rights of Data Subjects, as set out in GDPR, are observed correctly.

This Policy sets out the rights of the aforementioned individuals as Data Subjects and the processes which should be followed in the event that the Data Subject wishes to exercise any such right, to the extent of the Applicable law. This Policy applies internationally to Data Respons' processing of Personal Data concerning all Applicants, Employees, Suppliers and Business Partners, whether by electronic or manual means (i.e., in hard copy, paper, or analog form).

Policy statement

All Data Respons Group employees are required to comply with their obligations under the GDPR, in relation to personal data about other employees, candidates, suppliers, partners and customers. Employees in positions that require use of personal data will be given separate specific guidance on these obligations and appropriate training.

Employees must ask the Data Respons Data Protection Responsible in their organisation if they are unsure of their obligations.

If any employees fail to comply with these obligations, their failure will be regarded as a breach with the Company's Code of Conduct[1].

[1] https://www.datarespons.com/wp-content/uploads/2015/01/Data-Respons-Code-of-Conduct-eng.pdf

TABLE OF CONTENTS

1. Definitions

2. Responsibilities

3. Employees Data Protection

4. Customers and Partners Personal Data

5. Data Subject Rights

6. Transfer of Personal Data

7. Personal Data Processing Security

8. Monitoring Of Personal Data Protection Obligations

9. Personal Data Breaches and Data Protection incidents.

1. DEFINITIONS

"Data Respons" means Data Respons AS and any company or entity that is directly, indirectly or commonly controlled by Data Respons AS where control means either (i) direct or indirect ownership or control of more than 50% of the voting interests of the subject company or entity, or (ii) the ability to control the activities of the subject entity through contractual rights.

"Applicable Laws" means (a) European Union or EU Member State laws in respect of which you or Data Respons are subject to EU Data Protection Laws; and (b) any other applicable law in respect of which you or Data Respons are subject to any other Data Protection Laws;

"Customers, Suppliers and Business Partners" means Data Respons' customers, suppliers and business partners. These parties are most of the time legal entities. However, Data Respons processes Personal Data of their representatives, agents, staff members, employees and contact persons for the purposes set out in this Notice. Business Partners also include shareholders, associates and partners.

"Employee" means current and past members of the internal workforce who have a direct work contract with Data Respons, such as employees, temporary workers, interns, consultants and independent workers.

"Personal Data" means any information about an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, 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.

"Processing" or "Processed" means any operation or set of operations which is performed on Personal Data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Sensitive Data" means any information relating to an Employee's race or ethnic origin, political or philosophical opinions, religious beliefs, physical or mental health or condition, sexual life, preference or orientation, trade union membership or affiliation, biometric data used for the purpose of uniquely identifying an Employee, and genetic information.

2. RESPONSIBILITIES

It is the responsibility of all line managers to ensure that they understand and communicate this Personal Data Protection policy to employees dealing with personal data. It is the responsibility of each employee to ensure that they understand this policy. The Data Protection responsible for each entity or country ultimately has accountability for the operation and monitoring of this policy. Human Resources shall provide support to the Data Protection responsible when required and will ensure that issues are dealt with consistently, promptly and fairly.

Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any personal data processing is carried out in accordance with the GDPR.

Each Data Respons entity must identify their Data Protection responsible. The Data Protection responsible coordinates personal data protection for such entity, in cooperation with Data Respons management.

The responsibilities of the Data Protection Responsible include:

- Familiarize the employees with the content of the Data Respons Personal Data Protection policy.
- Promote the implementation and use of personal data processes and protection measures, in particular in case of processing of extremely sensitive personal data or transfers of personal data outside of the EEA.
- Ensure that their employees are sufficiently trained in personal data protection.
- Identify improper processing of personal data, or other violations of the data protection laws, and elaborate and escalate the necessary reports.

3. EMPLOYEES DATA PROTECTION

The following types of personal data may be held by a Data Respons entity, as appropriate:

3.1 Job applicants and Employees

Personal Data, as well agency workers and other third parties working on Data Respons' behalf:

- Identification Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images;
- Financial and tax-related information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock-options, stock purchase plan;
- Recruitment information: such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable);
- Employment administration information, such as employment and career history, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers;
- Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records;
- Details of Employees' whereabouts in Data Respons' location to the extent recorded by electronic card access systems;
- Details of IT and connection data to the Data Respons IT systems.

Data Respons processes Job applicants and Employees' Personal Data as well as agency workers and other third parties' working Data Respons' behalf exclusively for work-related purposes. Such purposes include but are not limited to the following activities:

- Recruitment, including background checks subject to Applicable laws,
- Performance assessment and training;
- Pay-roll and administration of other employment-related benefits (including stock-options, stock purchase plan, or other corporate plans or benefits);
- Day-to-day management activities, such as deployment on projects, promotion, disciplinary activities, grievance procedure handling;
- Marketing the professional services of consultants to potential clients (e.g., by providing details of experience on previous projects);
- Administration of current benefits, including the personal pension plan, life insurance scheme, private health insurance scheme;
- Employment analysis, for example, comparing the success of various recruitment and/or Employee retention programs;
- Compliance with health & safety rules and other legal obligations as an employer;
- Where necessary, processing designed to enable the exercise of legal rights, and/or perform its legal obligations, as an employer, in so far as it is required by Applicable Law of the country where a Data Respons' entity is responsible for the Personal Data;
- IT, security, cybersecurity and access control;
- Human Resource Management, Career management and mobility;

- Internal and external communication;
- Disaster recovery plan and crisis management;
- Company resources management;
- Audit and statistics.

3.2 Business Partners

Business Partners means Data Respons" supplier, subcontractor, shareholder, client or alliance partner, whether having an on-going commercial relationship with the Company or being a former or potential Business partner:

- Contact details, such as name, job title, employer, address, telephone numbers, e-mail address, fax numbers;
- Financial details relating to invoicing and payment, such as bank account information (when the Business Contact is a natural person);
- Relevant experience and/or qualifications (such as for the personnel of subcontractors);
- Details of business interests and opinions (such as where information is held in a CRM marketing database).

Data Respons processes Business partners' Personal Data exclusively for business related purposes. Such purposes include but are not limited to the following activities:

- Concluding and performing contracts with clients, suppliers, subcontractors or alliance partners;
- Managing accounts and records;
- Advertising, marketing and public relations;
- Communicating with Business Contacts;
- Market research;
- Health, Security, Environment and Quality;
- Compliance with legal and regulatory obligations;
- Maintaining certifications;
- Audit and statistics.

3.3 Why do we collect and on what legal basis do we collect personal data

Given Consent (Article 6, Section 1, lit. a) GDPR).

If personal data are processed based on consent given by you, you have the right to object to this consent at any time with future effect without giving specific reasons for that.

Processing based on legal requirements (Article 6 Section 1 lit. c) GDPR)

The Controller has the duty to comply and fulfill legal requirements (e.g. tax-related or commercial obligations and taxes)

Processing necessary for legitimate interests (Article 6, Section 1, lit. f) GDPR)

Additionally, we process your personal data to maintain the legitimate interests of our HR functioning, the business or third parties except where such interests are overridden by your

interests or fundamental rights and freedoms which require protection of personal data.

Sensitive Data that may be collected:

We do not request any Sensitive Data and therefore we kindly ask you to avoid from disclosing such information. Nonetheless, we may collect Sensitive Data, if authorized by law and where necessary to comply with Applicable laws or if you spontaneously provide it to us in your CV.

Nevertheless, if you are working for Data Respons, we may collect, store and use the following categories of Sensitive Data which will be collected and used only if and to the extent a local legislation requires it:

- information about your health, including any medical condition, health and sickness records, including:
- where it is needed for determination of working capacity based on health conditions:
- sick-leave records
- where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision
- where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

Personal Data disclosures

The Data Respons Entity may be required to disclose certain personal data to a third person. The circumstances leading to such disclosures include:

- Any employee benefits operated by third parties;
- Disabled employees - whether any reasonable adjustments are required to assist them at work;
- Employee's health data - to comply with health and safety or occupational health obligations towards the employee;
- For statutory Sick Pay purposes;
- HR management and administration - to consider how an employee's health;
- affects his or her ability to do their job;
- The smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Acknowledgement of data processing

Employees shall be informed of the Data Respons Personal Data Protection policy at the moment they enter into labour relationship with Data Respons. A copy of Data Respons Personal Data Protection Policy will be added to the employment contract and all necessary resources will be in place to ensure employees understand their rights and obligations under this policy.

4 CUSTOMER AND PARTNERS PERSONAL DATA

Data processing for a contractual relationship or advertising

Personal data of the relevant prospects, customers and partners can be processed to establish, execute and terminate a contract. Also, if a Data Subject contacts Data Respons to request information about a service or product, data processing to meet this request is permitted. If a Data Subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes.

Consent to Personal Data processing

In this case Personal Data for Customers and Partners can be processed following consent by the Data Subject. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

If personal data are collected, processed and used on websites or in apps, Data Subjects must be informed of this in a privacy statement and, if applicable, in the information about cookies If use profiles (tracking) are created to evaluate the use of websites and apps, the Data Subjects must always be informed accordingly in the privacy statement.

Personal tracking may only be effected if it is permitted under Applicable law or upon consent of the Data Subject. If tracking uses a pseudonym, the Data Subject should be given the chance to opt out in the privacy statement.

5 DATA SUBJECT RIGHTS

Under GDPR, all persons have the following rights in relation to their personal data:

- The right to be informed
- The right of access
- The right for any inaccuracies to be corrected
- The right to have information deleted
- The right to restrict the processing of the data
- The right to portability
- The right to object to the inclusion of any information
- The right to regulate any automated decision-making and profiling of personal data.

Right to be informed

Data Subjects have the right to be told how Data Respons processes their personal data and the reasons for the processing. Data Respons has developped this Data Respons Personal Data policy to explain what data will be collected, how Data Respons collects and processes it, what Data Respons processes it for and the lawful basis which permits Data Respons to process it.

Data Subjects can obtain a copy of this policy from our internal communication platform or via a local managing director. If Data Respons intends to use data already collected from a Data Subject for a different reason than that already communicated, Data Subject will be informed of the new reason in advance.

Right of access

Data Subjects have the right to access their personal data which is held by Data Respons. To request access to their personal data, Data Subjects can address their request to the following email address: data-protection@datarespons.com.

Right for data to be corrected or deleted

One of the fundamental principles underpinning data protection is that personal data which Data Respons processes about data Subjects are accurate and up to date. Data Subjects have the right to have their personal data corrected if it is inaccurate or incomplete. If a Data Subject wishes to have his/her data rectified, he/she should do so by sending a request to the following email address: data-protection@datarespons.com.

Data Subjects have the right to have their data deleted and removed from Data Respons systems where there is no compelling business reason for Data Respons to continue to process it.

Data Subjects have a right to have their personal data deleted in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which Data Respons originally collected or processed it
- where Data Subject have withdrawn his/her consent to the continued processing of the data and there is no other lawful basis for Data Respons to continue processing the data
- where Data Subject objects to the processing and Data Respons has no overriding

legitimate interest to continue the processing
- the personal data has been unlawfully processed
- the personal data has to be deleted due to a legal obligation. If the Data Subject wishes to make a request for data deletion, he/she should send a request to the following email address: data-protection@datarespons.com.

Upon receipt of a request, Data Respons will delete the data unless it is processed for one of the following reasons:

- To exercise the rights of freedom of expression and information
- For Data Respons to comply with a legal requirement
- The performance of a task carried out in the public interest or exercise of official authority
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific historical research or statistical purposes or
- The defence of legal claims.

Where the request of the Data Subject is not complied with because of the one of the above reasons, they will be informed of the reason. Where the request is to be complied with, the Data Subject will be informed when the data has been deleted.

Where the personal data which is to be deleted has been shared with third parties, Data Respons will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect or imply disproportionate costs for Data Respons, this notification may not be carried out.

Making a Data Subject access request

Data Subject access requests to their personal data must be made in writing to the following email address: data-protection@datarespons.com. Including specific details of the personal data that the Data Subject wishes to see will enable a more efficient response from Data Respons. Data Respons may need to contact the Data Subject for further details on their request if insufficient information is contained in the original request.

Data Respons will comply with the request without delay and at the latest within 30 working days from reception of the request unless one of the following applies:

In some cases, Data Respons will be unable to supply certain pieces of information requested. This may be because it is subject to legal privilege or relates to management planning. Where this is the case, Data Respons will inform the Data Subject that his/her request cannot be complied with, and an explanation of the reason will be provided.

If Data Respons requires extra time because the requests are complex or numerous, in these circumstances, Data Respons will write by replying the email sent by the Data Subject within one month of receipt of the request to explain why an extension is required. Where an extension is required, information will be provided within three months of the request.

Data Subject requests will normally be complied with free of charge. However, Data Respons may charge a reasonable fee if the request is manifestly unfounded or excessive, or if it is repetitive. In addition, Data Respons may charge a reasonable fee if the Data Subject requests further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested.

Data Respons may refuse to comply with a Data Subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, Data Respons will write to the Data Subject without undue delay and at the latest within one month of receipt to explain why Data Respons is unable to comply. Data Subject will be informed of the right to complain about that.

6 TRANSFER OF PERSONAL DATA

The Data Respons entity transfer personal data/information to another entity within the Data Respons Group, including to countries outside of the European Union, solely for purposes connected with the ongoing employment of the employee or efficient management of Data Respons' business activities.

Transfer of personal data to recipients within the Data Respons Group is subject to the authorization requirements for processing personal data under the Data Transfer Agreement (DTA) signed by all entities of the Data Respons Group. The data recipient must be required to use the data only for the defined purposes and under the terms of such DTA.

In the event that personal data are transmitted to a recipient within the Data Respons Group to a country located outside of the European Union or outside the European Economic Area, such entity must agree to maintain a personal data protection level equivalent to this Personal Data Protection Policy. If Personal data are transmitted by a third party outside of the Data Respons Group, it must be ensured that the processing of such data fulfils the conditions of this Personal Data Policy, or similar conditions that respect the GDPR obligations.

7 PERSONAL DATA PROCESSING SECURITY

Data Respons Group implements security measures to ensure the personal data processed is safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented.

8 DATA RETENTION

We only retain your Personal Data for as long as it is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, tax, insurance or reporting requirements and to safeguard the applicable statutes of limitations.

To determine the appropriate retention period for Personal Data, we consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorised use or disclosure of your Personal Data, the purposes for which we process your Personal Data and whether we can achieve those purposes through other means, and the applicable legal requirements.

For employees:
Once you are no longer working for the company, we will retain and securely destroy, delete or anonymize personal data in accordance with applicable laws and regulations.

For job applicants:
For all job applicants your personal data are processed based on your given consent and will, as described therein, be erased after 24 months according to the termination of the purpose. If you want your data to be stored beyond that time limit please answer to the mail, send to you shortly before the 24-month time period terminates.

Are your personal data processed based on your given consent and you object, this consent your personal data will be erased directly unless there are no other legal requirements that obligate us to store this specific data for a longer time.

If there are other existing legal obligations that require a longer retention period, we will apply the specific rules on data that are affected by that.

For third parties and business partners:

- Data Respon shall retain Personal Data only for the period reasonably necessary:
- to serve the purposes described in this Policy for which the Personal Data are processed, specifically, if we have an ongoing legitimate business need to do so (for example to provide you with a contractual service you have requested);
- to comply with applicable legal obligations (for example for financial, tax, accounting and insurance obligations);
- to safeguard the applicable statute of limitations (for examples with respect to contractual claims).

For contracts, the retention period is the term of your (or your company's) contract with us, plus the period until the legal claims under this contract become time-barred, unless overriding legal or regulatory schedules require a longer or shorter retention period. When the above retention periods expire, your personal data are removed from our systems.

9 MONITORING OF PERSONAL DATA PROTECTION OBLIGATIONS

Data Respons Personal Data Protection Policy is checked at local and group level and under the responsibility of the Data Protection Responsible of each entity and the Data Respons Group. The results of the data protection controls must be reported to the Data Respons Group Personal data responsible. This function is piloted by the Chief Communication Officer.

10 PERSONAL DATA BREACHES AND DATA PROTECTION INCIDENTS

All employees must inform immediately their supervisor, the Data Protection responsible in their entity or at Data Respons Group level, the local IT department or the Chief Communication Officer about breaches of this Personal Data Protection Policy and any protection incidents.

An internal report shall be completed to document any case of improper transfer of personal data to third parties, improper access by third parties to personal data, or the loss of personal data, in order to comply with the reporting duties.

11 CONTACT AND UPDATE

If you have any questions about how we process your Personal Data, please feel free to contact us by sending an email to data-protection@datarespons.com.

Data Respons may change this Policy as needed. When we update this Policy, we will take appropriate measures to inform you, consistent with the significance of the changes we make. You can see when this Policy was last updated by checking the “last updated” date displayed at the top of this Policy.