

# Privacy Policy

Last updated on June 8<sup>th</sup> of 2018.

We would like to inform our Partners that in accordance with the [General Data Protection Regulation](#) (GDPR, Regulation) adopted by the European Union, which is binding from 25 May 2018, changes take effect to further protect the personal data of individuals who come into contact with our company.

The Company performs the following data processing of external parties, the most important features of which are provided in this document.

The privacy policy also contains information on the rights of data subjects.

## **Data Controller:**

ÁTI DEPO Zrt is authorised to manage, store and process the data.

Company name::ÁTI Depo Közraktározási Zártkörűen Működő Részvénytársaság

Registered office: 1136 Budapest Pannónia street 11.

Contact person: Bonczó Ágnes

E-mail address: [adatvedelem@atidepo.hu](mailto:adatvedelem@atidepo.hu)

Court registration number: 01-10-043078

Tax Number: 11197755-2-41

## Data management with the consent of the data subject

Prior to the application of the Regulation, a significant part of the data processing was based on the consent of the data subject, voluntary data provision, which will be applied by the Company by a decreasing importance in the future, as the data processing has a different legal basis in many cases.

In the case of consent-based data processing, the data subject's consent to the processing of his or her personal data must be requested in advance.

Consent shall also be deemed to be the consent of the data subject, when the data subject indicates this by checking an applicable box at viewing the Company's website, or the data subject makes technical settings when using information society services, or the data subject makes any other statement or action, which clearly indicates his/her consent to the planned personal data processing in a given context..

The consent shall cover all data processing activities carried out for the same purpose or purposes. If the data management serves several purposes at the same time, the consent must be given for all data management purposes

If the data subject consents in a form of a written statement relating to other matters as well - for example the conclusion of a sales or service contract- the request for consent must be made in a way that is clearly distinguishable from those other matters, in a comprehensible and easily accessible manner with clear and simple language. Any part of such a statement containing the data subject's consent which infringes the Regulation shall not be binding.

The Company may not set as a condition of the conclusion or performance of a contract to give consent to the processing of personal data, that is not necessary for the performance of the contract.

Withdrawal of a consent should be allowed on a similarly simple way as the giving of the consent.

Child data may only be processed by the Company with the consent of a parent or guardian.

If the personal data was collected with the consent of the data subject, the data manager may, unless otherwise provided by law, process the collected data for the purpose of fulfilling the legal obligation without further consent and after the withdrawal of the data subject's consent.

The Company makes its privacy policy available to the data subjects on its website. The purpose of the privacy policy is to inform data subjects in a publicly available form clearly and in detail before and during the processing of all facts relating to the processing of their data. In particular about the purpose and legal basis of the processing, the person entitled to control and process data, the duration of the processing and about the fact if the personal data of the data subject are processed by the data controller in accordance with Infotv. § 6 (5) and about who can get acquainted with the data. The privacy policy should also cover the data subject's rights and remedies. This privacy policy must be made available by marking a separate link for each of the most important data management steps (for example, in the case of a registration before registration, during the registration process, etc.). Data subjects should be informed of the availability of this policy.

Data processing necessary for compliance with a legal obligation is independent of the data subject's consent, as the data processing is defined by law or by an authority. The data subject shall be informed before the start of the data processing that the data processing is obligatory and shall be clearly and in detail informed of all facts related to the processing, in particular the purpose and legal basis of the data processing, the person entitled to control and process data, the duration of the processing, whether the personal data of the data subject are processed by the data controller on the basis of the legal obligation applicable to him or her, and who can get acquainted with the data. The information should also cover the data subject's rights and remedies. In the case of mandatory data processing, the information may also be provided by publishing a reference to the legal provisions containing the above information.

### Processing of data of employees applying for hiring, applications, CVs

**The range of personal data that can be processed:** the natural person's name, date of birth, place, mother's name, address, qualification data, payment-related data, photo, telephone number, e-mail address, employer's record of the applicant (if any).

**The purpose of the processing of personal data:** application, assessment of the application, conclusion of an employment contract with the selected person. The person concerned must be informed if the employer has not chosen him/her for the job.

**Legal basis for data processing:** consent of the data subject.

**Recipients and categories of recipients of personal data:** the head of the Company entitled to exercise employer's rights, the head of the particular field, employees performing labor duties, a law firm in connection with legal representation and the implementation of legal matters, the ERP system support service provider, in connection with the internal and external support of IT operations tasks, the IT service provider, the service provider responsible for security.

**Duration of storage of personal data:** Until the application is considered. The personal data of non-selected candidates must be deleted at the latest after 6 months. The data of the person who withdrew his/her application must also be deleted.

The employer may retain applications only with the express, explicit and voluntary consent of the data subject, provided that their retention is necessary to achieve the purpose of data processing in accordance with the law. This consent must be requested from applicants once the recruitment procedure has been completed.

### Workplace, on-site entry and exit data processing

In case of operation of an access control system, information on the identity of the data controller and the manner of data processing shall be placed.

At each site, personal and vehicle access and physical security services are provided by external service providers. As part of this, vehicles may be inspected at the point of entry.

**The range of personal data that can be processed:** the name and address of the natural person, the registration number of the car, the time of entry and exit.

**The legal basis of data processing:** enforcing the legitimate interests of the employer and fulfilling the contractual obligation.

**The purpose of the processing of personal data:** protection of property and assets, performance of the contract, control of the fulfillment of employee obligations

**Recipients and categories of recipients of personal data:** the head of the Company entitled to exercise employer's rights, the head of the particular workplace or site manager, the employees of the security service provider, a law firm in connection with legal representation and the implementation of legal matters, the auditor, in connection with the site entry /exit the service provider responsible for security, in connection with the internal and external support of IT operations tasks, the IT service provider, the service provider responsible for security.

### Data processing related to camera surveillance

**Purpose of data processing:** The Company uses an electronic surveillance system at its registered office, countyside offices/sites and premises open to the reception of customers for the protection of human life, physical integrity, personal freedom, trade secrets and property (asset) protection, which uses image, sound or image and sound recording. also allows, on the basis of this, the behavior of the data subject, which is recorded by the camera, can also be considered as personal data.

**The legal basis of data processing:** the enforcement of the legitimate interests of the employer and the consent of the data subject (visitors, guests).

Before entering the camera recording zone, the data subject's attention must be drawn to the fact of the recording (primary information) using a clearly visible pictogram. A warning sign, information on the fact of the use of the electronic surveillance system in a given area shall be placed in a clearly visible place, in a clearly legible manner that facilitates the information of third parties wishing to enter the area (detailed written information). This information shall include the fact of the surveillance is carried out by the electronic security system and the purpose of making and storing the image and sound recording - containing personal data - , the legal basis of data processing, the place of storage, the duration of storage, identification of the system operator (operator), on the identification of persons having access to the personal information, as well as the provisions concerning the rights of the data subjects and the procedure for their enforcement.

**Scope of data processed:** camera images and moving image recordings of the data subjects, the movements of the data subject, and for some cameras, a detailed face and body image of the data subject.

Images and audio recordings of third parties (customers, visitors, guests) entering the monitored area can be taken and processed with their consent. Consent may also be given by implied conduct. Indicative behavior, in particular, if the natural person acknowledging any sign, information on the use of camera surveillance system, enters to the particular area.

**Duration of personal data storage:** the recorded recordings can be stored for a maximum of 3 (three) working days if they are not used. Use is defined as the use of recorded video, sound or image and sound recordings and other personal data as evidence in court or other official proceedings.

A person whose right or legitimate interest is affected by the recording of image, sound or image and sound recording data may, within three working days from the recording of the image, sound and image and sound recording, request – certifying his/her right or legitimate interest-, that the data must not be destroyed or deleted by its operator.

An electronic monitoring system may not be used in premises where surveillance may infringe human dignity, in particular in changing rooms, showers, toilets or, for example, in a medical premise or its waiting room, or in premises set aside for workers' breaks.

If no one is legally present in the workplace, especially outside working hours or on public holidays, the entire workplace (such as changing rooms, toilets, breaks) can be observed..

**Recipients and categories of recipients of personal data:** In addition to those authorized by law, the operators, the head and deputy employer and the workplace manager of the monitored

area are entitled to view the data recorded by the electronic surveillance system in order to detect violations and control the operation of the system, a law firm in connection with legal representation and the implementation of legal matters, the auditor, in connection with the viewing of the camera images the service provider responsible for security, in connection with the internal and external support of IT operations tasks, the IT service provider, the service provider responsible for security.

## CONTRACT - RELATED DATA PROCESSES

### Management of data of contracting partners - registration of customers, suppliers, other partners and contacts

**Legal basis for data processing:** Data processing is necessary for the performance of a contract in which the data subject is required by one of the parties or to take steps at the request of the data subject prior to the conclusion of the contract (Article 6 (1) (b) of the Regulation). or for enforcing the the legitimate interests of the company (Article 6 (1) (f) of the Regulation )and compliance with a legal obligation.

The Company manages the name, birth name, date of birth, mother's name, address, tax identification number, tax number, sole enterprenaour/primary private agriculture producer ID number, EORI and VPID number, ID card number, address card number, registered office/site address, telephone number, fax number, e-mail address, website address, bank account number, customer number (eg client number, order number ), license plate number, online ID and the declaration on infectious disease of the private persons entering the Baja site (as part of the documentation re GMP+ B3 (2007) standard) of the natural person contracted as a partner, a natural person related to a legal or non-legal person or organization, or a witness signing certain documents the name **for the purpose** of concluding, fulfilling, terminating the contract and providing a contractual discount.

Typical cases of this type of data processing: handing over a business card, conducting a business negotiation, requesting a business offer, submitting a business offer, requesting and sending contract or order (hereinafter: contract) data, performing a contract, proving the fulfillment of a contract, entering the Baja site.

Such data processing is also lawful if the data processing is necessary to take steps at the request of the data subject prior to the conclusion of the contract.

**Recipients and categories of recipients of personal data:** employees of the Company performing customer service tasks, security service provider, employees and service provider of the company performing accounting, auditing and taxation tasks, a law firm in connection with legal representation and the implementation of legal matters, the ERP system support service provider, the auditor, in connection with the internal and external support of IT operations tasks, the IT service provider, the service provider responsible for security, the authorities requesting / receiving documents including personal data, and the GMP auditor.

**Duration of storage of personal data:** the scope of the data stored must be reviewed by 30th of September, each year subsequent to the start of processing, and the relevant data are deleted after 8 years, or 5 years in the case of a GMP declaration. Otherwise, the period of time specified in the data processing legislation or the period of time for which the processing of data is necessary for the enforcement of a legitimate interest.

The data subject must be informed informally before the start of the data processing that the data processing is based on the performance of the contract, the relevant part of the contract can be used as an evidence for this information provision

[Details of natural person representatives of legal entity clients, customers, suppliers or other partners](#)

**The range of personal data that can be processed:** the name, address, telephone number, e-mail address and online ID of the natural person.

**Purpose and legal basis of the processing of personal data:** fulfillment of the contract concluded with the Company's legal entity partner, business relations, with the voluntary consent of the representative person

**Recipients and categories of recipients of personal data:** employees and service provider of the Company performing customer service tasks, a law firm in connection with legal representation and the implementation of legal matters, the ERP system support service provider, the auditor, in connection with the internal and external support of IT operations tasks, the IT service provider, the service provider responsible for security.

**Duration of storage of personal data:** regarding the business relations and the contacts as data subjects the period of time specified in the data processing legislation or the period of time for which the processing of data is necessary for the enforcement of a legitimate interest.

This statement must be communicated by the employee related to the client, supplier to the person concerned. The statement shall be kept for the duration of the processing.

[Data processing regarding visitors on the Company's website - Information on the use of cookies](#)

The Company's websites serve to inform partners and visitors and contain a suitable function for initiating contact. In this case, the visitor can use the Contact or Request for Quotation subpages and submit a request to customer service by entering their details voluntarily.

Websites use cookies in order to facilitate the use of the internet service and make it more convenient to use the website. Cookies are short data files that are placed on the user's computer by the website you are visiting. There are many varieties, but they can generally be classified into two major groups. One is a temporary cookie that a website places on a user's device only during a particular session, and the other type is a persistent cookie (e.g., a website's language setting) that remains on the computer until the user deletes it. According to the guidelines of the European Commission, cookies (unless they are absolutely necessary for the use of the given

service) may only be placed on the user's device with the user's permission. Information about this and asking for the user's consent is provided by a message at the bottom of the website.

In the case of cookies that do not require the user's consent, information must be provided during the first visit to the website. It is not necessary for the full text of the cookie information to appear on the website, it is sufficient for the website operators to briefly summarize the essence of the information and to indicate the availability of the full information via a link.

In the case of cookies requiring consent, the information may also be related to the first visit to the website in the event that the data processing associated with the use of cookies begins with a visit to the website. If the use of a cookie is related to the use of a function specifically requested by the user, the information may also be displayed in connection with the use of this function. In this case, it is not necessary for the full text of the cookie information to appear on the website, a short summary of the essence of the information and a reference to the availability of the full information leaflet will suffice.

The visitor must be informed about the use of cookies on the website in the privacy policy. With this information, the Company ensures that the visitor can find out the purposes of the data processing by the Company, the types of the data processed, including the handling of data that cannot be directly linked to the user, anytime before and during the use of the information society-related services of the website.

**The purpose of the personal data processing functions** of the website is to facilitate the operation of the website and to facilitate contact.

**Legal basis for data processing:** performance of the contract and voluntary consent of the visitor

**Scope of data processed:** The given name, email address, telephone number, and the following cookie types: tracking cookie.

**Duration of storage of personal data:** the scope of the data provided must be reviewed by the 30th of September, each year, subsequent to the start of treatment and deleted after 8 years. Static cookies can be cleared by the user by clearing the browser cache, and session cookies are cleared when the browser window is closed

**Recipients and categories of recipients of personal data:** employees of the Company performing customer service tasks, service provider of the company performing accounting, auditing and taxation tasks, law firm in connection with legal representation and the implementation of legal matters, the auditor, in connection with the internal and external support of IT operations tasks, the IT service provider, website hosting provider, the service provider responsible for security. Web page service tasks are performed by Wix.com Ltd.

## DATA PROCESSING RE LEGAL OBLIGATIONS

Data processing, necessary for compliance with tax-, accounting and other legal or regulatory purposes

The Company manages the data as defined in the regulation of natural persons who enter into business relations with it as a partner **for the purpose of fulfilling a legal obligation**, to fulfill statutory tax, accounting and other legal or official obligations (accounting, taxation, provision of data). The data managed are in particular as per sections § 169 and § 202 of Act of CXXVII. 2017 on value added tax: : tax number, name, address, tax status, as per § 167 of Act C. 2000 on Accounting: name, address, indication of the person or organization ordering the economic transaction, the signature of the person approving the transaction, depending on the organization, the signature of controller, on the documents of stock and cash movements, the signature of the recipient, on the counter-receipts the signature of the payer, as per the personal income tax Act CXVII. 1995.: business card ID, number of primary producer card, sole enterprenaour/primary private agriculture producer ID, tax identification number.

**The period of storage of personal data:** is 8 years after the termination of the legal relationship giving rise to the legal basis.

**Recipients and categories of recipients of personal data:** the Company's employees and service providers performing tax, accounting, auditing, payroll, social security and data provision tasks, law firm in connection with legal representation and implementation of legal matters, ERP system support service provider, auditors, in connection with the internal and external support of IT operation tasks, the IT service provider, the service provider responsible for security, the data requesting authority.

Data management for the purpose of meeting anti - money laundering obligations

**In order to fulfill its legal obligation**, the Company manages personal data defined in Act LIII. 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing for the purpose of fulfilling and preventing money laundering and terrorist financing (Pmt.) and Act CXCVI of 2011 Act on national property., such as : surname and first name of a natural person, surname and first name of birth, nationality, place of birth, time, mother's birth name, address, failing which place of residence, type and number of identification document; the number of the official identity card certifying the address, a copy of the presented documents. (§ 7 (8.)) of its clients, their representatives and the beneficial owners.

**Recipients and categories of recipients of personal data:** the Company's employees and service providers performing customer service-related tasks, the head of the Company's and the designated person of the Company's as per Pmt., the project manager, in connection with the internal and external support of IT operation tasks, the IT service provider, the service provider responsible for security.

**The period of storage of personal data** is 8 years from the termination of the business relationship or the execution of the transaction order. (Section 56 (2) of the Pmt.)



## Information on the rights of the data subjects

### Right to advance information

The data subject has the right to be informed of the facts and information related to the data processing before the data processing starts.

### Information to be provided if personal data are collected from the data subject

If personal data concerning the data subject are collected from the data subject, the controller shall provide the data subject with all of the following information at the time the personal data are obtained:

- the identity and contact details of the controller and, if any, the controller's representative;
- the contact details of the Data Protection Officer, if any;
- the purpose of the planned processing of personal data and the legal basis for the processing;
- in the case of data processing based on Article 6 (1) (f) of the Regulation (enforcement of a legitimate interest), the legitimate interests of the controller or of a third party;
- where applicable, the recipients of the personal data or the categories of recipients, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or an international organization, and the existence or absence of a Commission decision on adequacy, or in the case of data transmission as per Articles 46, 47 or second subsection of 49 (1) of the Regulation, the indication of the appropriate and suitable guarantees and a reference to the means of obtaining or obtaining a copy thereof.

In addition to the information referred to above, the controller shall provide the data subject with the following additional information at the time the personal data are obtained, in order to ensure fair and transparent data processing:

- the duration of the storage of personal data or, if this is not possible, the criteria for determining this period;
- the data subject's right to request the controller to access, rectify, delete or restrict the processing of personal data concerning him or her and to object to the processing of such personal data and the data subject's right to data portability;
- the right to withdraw the consent at any time in the case of data processing based on Article 6 (1) (a) (consent of the data subject) or Article 9 (2) (a) (consent of the data subject) of the Regulation, which does not affect the lawfulness of the data processing carried out on the basis of the consent prior to the withdrawal;
- the right to submit a complaint with the supervisory authority;
- whether the provision of personal data is based on a law or a contractual obligation or a precondition for concluding a contract, whether the data subject is obliged to provide personal data and the possible consequences of non-disclosure;
- the fact of the automated decision-making referred to in Article 22 (1) and (4) of the Regulation (if it is performed), including profiling, and, at least in these cases,

comprehensible information on the logic used and the significance of the expected consequences of these to the data subject

If the controller intends to carry out further processing of personal data for a purpose other than that for which they were collected, it shall inform the data subject of that different purpose and of any relevant additional information referred to in paragraph 2 before further processing.

The above shall not apply if and to the extent that the data subject already has the information. (Article 13 of the Regulation)

#### Information to be provided if personal data have been obtained not from the data subject

If the personal data have been obtained from others than the data subject, the controller shall provide the data subject with the following information:

- the identity and contact details of the controller and, if any, the controller's representative;
- the contact details of the Data Protection Officer, if any;
- the purpose of the planned processing of personal data and the legal basis for the processing;
- the categories of personal data concerned;
- the recipients of the personal data and the categories of recipients, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or an international organization, and the existence or absence of a Commission decision on adequacy, or in the case of data transmission as per Articles 46, 47 or second subsection of 49 (1) of the Regulation, the indication of the appropriate and suitable guarantees and a reference to the means of obtaining or obtaining a copy thereof.

In addition to the information referred to in the previous point, the controller shall provide the data subject with the following additional information necessary to ensure fair and transparent data processing for the data subject:

- the duration of the storage of personal data or, if this is not possible, the criteria for determining this period;
- if the processing is based on Article 6 (1) (f) of the Regulation (legitimate interest), the legitimate interests of the controller or of a third party;
- the data subject's right to request from the controller access to, rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of personal data, as well as the data subject's right to data portability;
- the right to withdraw consent at any time in the case of data processing based on Article 6 (1) (a) (consent of the data subject) or Article 9 (2) (a) (consent of the data subject) of the Regulation, which does not affect the lawfulness of the data processing carried out on the basis of the consent prior to the withdrawal;
- e) the right to submit a complaint with a supervisory authority;
- (f) the source of the personal data and, where applicable, whether the data come from publicly available sources; and

- (g) the fact of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) of the Regulation (if it is performed), and at least in such cases, understandable information on the logic used and the significance of such data processing and the expected consequences on the data subject. .

The data controller shall provide the information according to the previous points as follows:

- taking into account the specific circumstances of the processing of personal data, within a reasonable time from the receipt of the personal data, but no later than one month;
- if the personal data are used for the purpose of contacting the data subject, at least at the time of the first contact with the data subject;
- if the data is expected to be communicated to another recipient, at the latest when the personal data are first communicated.

If the controller intends to carry out further processing of personal data for a purpose other than that for which they were obtained, it shall inform the data subject of this different purpose and of any relevant additional information referred to in point 2 before further processing.

The preceding paragraphs shall not apply if and to the extent that:

- the data subject already has the information;
- the provision of such information proves impossible or would require a disproportionate effort, in particular for data processing for the purposes of archiving in the public interest, scientific and historical research or statistics, subject to the conditions and guarantees of Article 89 (1) of the Regulation, or where the obligation referred to in paragraph 1 of this Article is likely to make it impossible or seriously jeopardize the achievement of the purposes of such processing. In such cases, the controller shall take appropriate measures, including making the information publicly available, to protect the rights, freedoms and legitimate interests of the data subject;
- the acquisition or disclosure of the data is explicitly required by the applicable EU or Member State law, which provides for appropriate measures to protect the legitimate interests of the data subject; or
- personal data must remain confidential under an obligation of professional secrecy imposed by EU or Member State law, including a legal obligation of confidentiality. (Article 14 of the Regulation)

### Right of access by the data subject

The data subject has the right to receive feedback from the Data Controller as to whether the processing of his / her personal data is in progress and, if such data processing is in progress, he / she has the right to access the personal data and the following information:

- the purposes of data management;
- the categories of personal data concerned;

- the recipients or categories of recipients to whom or with whom the personal data have been or will be communicated, including in particular third country recipients or international organizations;
- where applicable, the intended period of storage of the personal data or, if this is not possible, the criteria for determining this period;
- the data subject's right to request the Data Controller to rectify, delete or restrict the processing of personal data concerning him or her and to object to the processing of such personal data;
- the right to submit a complaint with a supervisory authority;
- if the data were not collected from the data subject, all available information on their source;
- the fact of the automated decision-making referred to in Article 22 (1) and (4) of the Regulation (if it is performed), including profiling, and, at least in these cases, comprehensible information on the logic used and the significance of such data processing and the expected consequences on the data subject.

Where personal data are transferred to a third country or to an international organization, the data subject is entitled to be informed of the appropriate guarantees for the transfer in accordance with Article 46 of the Regulation.

The Data Controller shall provide the data subject with a copy of the personal data. The Data Controller may charge a reasonable fee based on administrative costs for additional copies requested by the data subject. If the data subject has submitted the request electronically, the information shall be provided in a widely used electronic format, unless the data subject requests otherwise. The right to request a copy must not adversely affect the rights and freedoms of others. (Article 15 of the Regulation)

### Right to erasure ("right to be forgotten")

The data subject has the right to obtain from the controller the erasure of personal data concerning him / her without undue delay at his / her request, and the data controller is obliged to erase the personal data concerning the data subject without undue delay if one of the following grounds applies:

- personal data are no longer required for the purpose for which they were collected or otherwise processed;
- the data subject withdraws his or her consent under Article 6 (1) (a) or Article 9 (2) (a) of the Regulation and there is no other legal basis for the processing;
- the data subject objects to the processing pursuant to Article 21 (1) of the Regulation and there is no overriding legitimate reason to process the data, or the data subject objects to the processing pursuant to Article 21 (2);
- personal data has been processed unlawfully;
- personal data must be erased in order to fulfill a legal obligation under EU or Member State law applicable to the Data Controller;
- personal data have been collected in connection with the provision of information society services referred to in Article 8 (1) of the Regulation.

Where the Data Controller has disclosed personal data and is required to erase it pursuant to paragraph 1 above, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the Data Controllers that the the data subject has requested them to delete the links to the personal data in question or a copy or duplicate of that personal data.

The above points do not apply if data management is required:

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.

### Right to restrict data processing

The data subject has the right to obtain from the controller restriction of processing if any of the following is met:

- the data subject disputes the accuracy of the personal data, in which case the restriction applies to the period of time that allows the Data Controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the data and instead requests that their use be restricted;
- the Data Controller no longer needs the personal data for the purpose of data processing, but the data subject requests them in order to submit, enforce or protect legal claims; or
- the data subject has objected to the processing in accordance with Article 21 (1) of the Regulation; in this case, the restriction shall apply for the period until it is determined whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the data subject

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted. (Article 18.)

### Right to data portability

The data subject shall have the right to receive personal data concerning him or her made available to a Data Controller in a structured, commonly used machine-readable format and to transfer such data to another Data Controller without being hindered by the Data Controller whose provided personal data if:

- the processing is based on a consent under Article 6 (1) (a) or Article 9 (2) (a) of the Regulation or a contract under Article 6 (1) (b); and
- data management is automated.

In exercising the right to data portability under point 1, the data subject shall have the right, if technically feasible, to request the direct transfer of personal data between Data Controllers.

The exercise of this right shall be without prejudice to Article 17 of the Regulation. That right shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the Data Controller.

The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others. (Article 20 of the Regulation)

### Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e, data processing is necessary for the performance of a task in the public interest or in the exercise of a public authority conferred on the Data Controller) or (f, the data processing is necessary to enforce the legitimate interests of the Data Controller or a third party) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for the purpose of direct business acquisition, the data subject shall have the right to object at any time to the processing of personal data concerning him for that purpose, including profiling, in so far as it relates to direct business acquisition.

If the data subject objects to the processing of personal data for the purpose of direct business acquisition, the personal data may no longer be processed for this purpose.

The right referred to in the preceding points shall be expressly brought to the attention of the data subject at the latest at the time of first contact and shall be displayed clearly and separately from all other information.

In connection with the use of information society services and by way of derogation from Directive 2002/58 / EC, the data subject may also exercise the right to object by automated means based on technical specifications.

Where personal data are processed for scientific and historical research or statistical purposes in accordance with Article 89 (1) of the Regulation, the data subject shall have the right to object to the processing of personal data concerning him or her on grounds relating to his or her situation, unless data management is necessary for the performance of a task performed in the public interest. (Article 21 of the Regulation)

### Automated individual decision-making, including profiling

The data subject shall have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have legal effects on him or her or would be similarly significant.

The preceding point shall not apply if the decision:

- necessary for the conclusion or performance of a contract between the data subject and the Data Controller;
- is made possible by EU or Member State law applicable to the Data Controller, which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or
- is based on the express consent of the data subject.

In the cases referred to in the first and last points of the previous point, the Data Controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including at least the data subject's right to request human intervention, express his or her views and object to the decision.

The decisions referred to in the second subparagraph may not be based on the specific categories of personal data referred to in Article 9 (1) of the Regulation, except where Article 9 (2) (a) or (g) applies and the rights, freedoms and legitimate interests of the data subject and appropriate measures have been taken to protect the interests of (Article 22 of the Regulation)

### Restrictions

Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 of the Regulation, as well as Article 5 of the Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 of the Regulation, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security,
- defence,
- public security,
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,

- other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security,
- the protection of judicial independence and judicial proceedings,
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in the first, fifth and seventh points,
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

The legislative measures referred to in the first subparagraph shall, where appropriate, include detailed provisions on at least:

- the purposes of the processing or categories of processing
- the categories of personal data,
- the scope of the restrictions introduced,
- the safeguards to prevent abuse or unlawful access or transfer,
- the specification of the controller or categories of controllers;
- the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing,,
- the risks to the rights and freedoms of data subjects; and
- the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction. (Section 23 of the Regulation).

### Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;



- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met. (section 34 of the Regulation)

#### Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78. (section 77 of the Regulation)

#### Right to an effective judicial remedy against a supervisory authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court. (section 87 of the Regulation)

#### Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers. (section 079 of the Regulation)