Personal Data Protection Policy
The Frontend Company

We at The Frontend Company are committed to processing personal data securely and respecting privacy of the concerned individuals.

Version No. and date of the last update:	v. 1.0. July 29, 2024
Approved by:	Oleksandr Vasylenko, CEO of The Frontend Company
This policy shall be reviewed annually or each time when the changes in our data processing occur.	

Table of contents

1. Scope and Definitions…….. 3
2. Data Processing Principles…… 6
3. Access to Personal Data. Legal Grounds and Purposes……. 8
4. Third Parties……. 10
5. International Transfers……. 11
6. Rights of Data Subjects……. 12
7. New Data Processing Activities…….. 17
8. Data Retention……... 19
9. Security……... 19
10. Data Breach Response Procedure……. 20

1. Scope and Definitions

1.1. **Scope**. This Personal Data Protection Policy (the "**Policy**") describes The Frontend Company internal rules for personal data processing and protection. The Policy applies to The Frontend Company, including The Frontend Company employees and contractors ("**we**", "**us**", "**our**", "**The Frontend Company**"). The management of each entity is ultimately responsible for the implementation of this policy, as well as to ensure, at entity level, there are adequate and effective procedures in place for its implementation and ongoing monitoring of its adherence. For the purposes of this Policy, employees and contractors are jointly referred to as the "**employees**".

1.2. **Privacy Manager**. Privacy Manager is an employee of The Frontend Company responsible for personal data protection compliance within The Frontend Company (the "**Privacy Manager**"). The Privacy Manager is in charge of performing the obligations imposed by this Policy and supervising other employees, who subject to this Policy, regarding their adherence to this Policy. The Privacy Manager must be involved in all projects at an early stage in order to take personal data protection aspects into account as early as the planning phase.

The designated Privacy Manager at The Frontend Company is Oleksandr Vasylenko.

1.3. **EU Representative**. As an entity processing personal data in accordance with the EU's legislation but located outside of the European Union, The Frontend Company must appoint the representative within one of the EU Member States. The task of the representative is to be a contact point for, including but not limited to supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

The appointed EU Representative of The Frontend Company is Oleksandr Vasylenko.

1.4. **Definitions**.

Competent Supervisory Authority	means a public authority that is responsible for regulating and supervising personal data protection with regards to activities of The Frontend Company.
Data Breach	means a breach of the security and/or confidentiality leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. This includes but is not limited to e-mails sent to an incorrect or disclosed list of recipients, an unlawful publication of the Personal Data, loss or theft of physical records, and unauthorized access to personal information.
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines (make a decision) the purposes and means of the processing of Personal Data.
Data Processor	means a natural or legal person, public authority, agency or other body which processes the Personal Data on behalf of the data controller.

Data Protection Laws	mean any laws and legal rules on personal data use and protection applicable to the activities of The Frontend Company, including, but not limited to the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).
Data Subject Request (DSR)	means any request from the Data Subject and concerning their personal data and/or data subject rights.
Data Subject	means a natural person, whose Personal Data we process. Data Subjects include but are not limited to users, website visitors, employees, contractors, and partners of The Frontend Company.
Personal Data	means any information relating to an identified or identifiable Data Subject; a Data Subject can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or the combination of factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject.
Processing	means any operation or set of operations which is performed by The Frontend Company on Personal Data, 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.
Standard Contractual Clauses	means the European Commission Decision of February, 5 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).
Third Party	means a natural or legal person, who accesses the Personal Data for further processing and is not an employee, member or corporate affiliate of The Frontend Company. This definition does not apply to natural persons, who provide services to The Frontend Company as contractors on a regular basis.
User	means a Data Subject who uses our services provided on The Frontend Company website.

2. Data Processing Principles

2.1. The Frontend Company's processing activities must be in line with the principles specified in this Section. The Privacy Manager must make sure that The Frontend Company's compliance documentation, as well as data processing activities, are compliant with the data protection principles.

2.2. We must process the Personal Data in accordance with the following principles:

2.2.1. Lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**). We shall always have a legal ground for the processing (described in Section 3 of this Policy), collect the amount of data adequate to the purpose and legal grounds, and we make sure the Data Subjects are aware of the processing;

2.2.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**). We must not process the Personal Data for the purposes not specified in our compliance documentation without obtaining specific approval of the Privacy Manager;

2.2.3. Adequate, relevant and limited to what is necessary for the purposes for which they are processed (**data minimization**). We always make sure the data we collect is not excessive and limited by the strict necessity;

2.2.4. Accurate and, where necessary, kept up to date (**accuracy)**. We endeavor to delete inaccurate or false data about Data Subjects and make sure we update the data. Data Subjects can ask us for a correction of the Personal Data;

2.2.5. Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed (**storage period limitation**). The storage periods must be limited as prescribed by Data Protection Laws and this Policy; and

2.2.6. Process in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures (**confidentiality, integrity, and availability**).

2.3. **Accountability**.

2.3.1. We shall be able to demonstrate our compliance with Data Protection Laws (**accountability principle**). In particular, we must ensure and document all relevant procedures, efforts, internal and external consultations on personal data protection including:

- the fact of appointing a person responsible for The Frontend Company's data protection compliance;
- where necessary, a record of a Data Processing Impact Assessment;
- developed and implemented notices, policies, and procedures, such as Privacy Notice, this policy or Data Breach response procedure;
- the fact of staff training on compliance with Data Protection laws; and

- assessment, implementation, and testing organizational and technical data protection measures.

2.3.2. The Privacy Manager must maintain The Frontend Company's Records of processing activities, which is an accountability document that describes personal data processing activities of The Frontend Company, prepared in accordance with Art. 30 of the GDPR (the "**Records of processing activities**"). The Records of processing activities must maintain, at least, the following information about each processing activity:

- contact details of The Frontend Company, the EU Representative, and, where applicable, of the Data Protection Officer;
- name of the activity, its purposes and legal basis along with, where applicable, the legitimate interests of The Frontend Company;
- data subjects and personal data categories concerned;
- data retention periods;
- general description of applicable security measures;
- recipients, including joint controllers, processors, and contractors involved, as well as the fact of the international data transfer with the safeguards applied to the transfer;
- where applicable, a reference to the Data Processing Impact Assessment;
- where applicable, a reference to the record of the data breach occurred involving the personal data;
- if The Frontend Company acts as a data processor, the information to be provided includes the names and contact details of controllers, name and contact details of controller's representative (if applicable), categories of processing (activities), names of third countries or international organizations that personal data are transferred to (if applicable), safeguards for exceptional transfers of personal data to third countries or international organizations (if applicable), and general description of technical and organizational security measures.

3. Access to Personal Data. Legal Grounds and Purposes

3.1. **Legal grounds**.

3.1.1. Each processing activity must have one of the lawful grounds specified in this Section to process the Personal Data. If we do not have any of the described, we cannot collect or further process the Personal Data.

3.1.2. If The Frontend Company is intended to use personal data for other purposes than those specified in the Records of processing activities, the Privacy Manager must evaluate, determine, and, if necessary, collect/record the appropriate legal basis for it.

3.1.3. **Performance of the contract**. Where The Frontend Company has a contract with the Data Subject, e.g. website's Terms of Use or the employment contract, and the contract requires the provision of personal data from the Data Subject, the applicable legal ground will be the performance of the contract.

3.1.4. **Consent**. To process the personal data based on the consent, we must obtain the consent before the Processing and keep the evidence of the consent with the records of Data Subject's Personal Data. The Privacy Manager must make sure that the consent collected from Data Subjects meet the requirements of Data Protection Laws and this Policy. In particular, the Privacy Manager must make sure that:

- the Data Subject must be free to give or refuse to give consent.
- the consent is in the form of an active indication from the Data Subject, i.e., the consent checkbox must not be pre-ticked for the user.
- the request for the consent clearly articulates the purposes of the processing, and other information specified in Subsection 6.2 is available to the Data Subject.
- the Data Subject must be free to give one's consent or to revoke it.

3.1.5. **Legitimate interests**. We have the right to use personal data in our 'legitimate interests'. The interests can include the purposes that are justified by the nature of our business activities, such as the marketing analysis of personal data. For The Frontend Company to use legitimate interests as a legal ground for the processing, the Privacy Manager must make sure that:

- the legitimate interest in the processing is clearly defined and recorded in the Records of processing activities;
- any envisaged risks to Data Subject rights and interests are spotted. The examples of the risks can be found in Subsection 7.2.;
- the Data Subjects have reasonable expectations about the processing, and additional protective measures to address the risks are taken;
- subject to the conditions of Subsection 6.7 (Right to object against the processing), the Data Subject is provided with the opportunity to opt-out from the processing for the described legitimate interests.

If at least one of the above conditions is not met by The Frontend Company, the Privacy Manager must choose and propose a different legal ground for the processing, such as consent.

3.1.6. **Legal Compliance and Public Interest**. Besides the grounds specified afore, we might be requested by the laws of the European Union or laws of the EU Member State to process Personal Data of our Users. For example, we can be required to collect, analyze, and monitor the information of Users to comply with financial or labor laws.

Whenever we have such an obligation, we must make sure that:

- we process personal data strictly in accordance with relevant legal requirements;
- we do not use or store the collected Personal Data for other purposes than legal compliance; and
- the Data Subjects are properly and timely informed about our obligations, scope, and conditions of personal data processing.

Important: Where The Frontend Company has the law requirements of another country to process personal data, the Privacy Manager must propose using

another legal ground for the processing under Data Protection Laws, such as legitimate interests or consent.

3.2. **Access to Personal Data**.

3.2.1. The employees must have access to the personal data on a "need-to-know" basis. The data can be accessed only if it is strictly necessary to perform one of the activities specified in the Records of processing activities. The employees and contractors shall have access to the Personal Data only if they have the necessary credentials for it.

3.2.2. Heads of the departments within The Frontend Company are responsible for their employees' access and processing of personal data. The heads must maintain the list of employees that are entitled to access and process personal data. The Privacy Manager shall have the right to review the list and, where necessary, request the amendments to meet the requirements of this Policy.

3.2.3. Heads of the departments within The Frontend Company must ensure that the employees under their supervision are aware of the Data Protection Laws and comply with the rules set in this Policy. To make sure our employees are able to comply with the data protection requirements, we must provide them with adequate data protection training.

3.2.4. All employees accessing personal data shall keep strict confidentiality regarding the data they access. The employees that access personal data must use only those means (software, premises, etc.) for the processing that were prescribed by The Frontend Company. The data must not be disclosed or otherwise made available out of the management instructions.

3.2.5. The employees within their competence must assist The Frontend Company's representatives, including the Privacy Manager, in any efforts regarding compliance with Data Protection Laws and/or this Policy.

3.2.6. When an employee detects or believes there is suspicious activity, data breach, non-compliance with Data Protection Laws and/or this Policy, or a DSR was not routed to the competent department within The Frontend Company, the employee must report such activity to the Privacy Manager.

3.2.7. Employees that are unsure about whether they can legitimately process or disclose Personal Data must seek advice from the Privacy Manager before taking any action.

3.2.8. Any occasional access to personal data for activities not specified in the Records of processing activities is prohibited. If there is a strict necessity for immediate access, the Privacy Manager must approve the access first.

4. Third Parties

4.1. Before sharing personal data with any person outside of The Frontend Company, the Privacy Manager must ensure that this Third Party has an adequate data protection level and provide sufficient data protection guarantees in accordance with Data Protection Laws, including, but not limited to the

processorship requirements (Art. 28 of the GDPR) and international transfers compliance (Section 5 of the GDPR). Where necessary, the Privacy Manager must make sure that The Frontend Company enters into the appropriate data protection contract with the third party.

4.2. An employee can share personal data with third parties only if and to the extent that was directly prescribed by the manager and specified in the Records of processing activities.

4.3. If we are required to delete, change, or stop the processing of the Personal Data, we must ensure that the Third Parties, with whom we shared the Personal Data, will fulfill these obligations accordingly.

4.4. Whenever The Frontend Company is engaged as a data processor on behalf of another entity, the Privacy Manager must make sure The Frontend Company complies with the processorship obligation. In particular, the appropriate data processing agreement in accordance with the Data Protection Laws must be in place. The Privacy Manager must supervise the compliance with data processing instructions from the controller, including regarding the scope of processing activities, involvement of sub-processors, international transfers, storage, and further disposal of processed personal data. The personal data processed under the processor role must not be processed for any other purposes than specified in the relevant instructions, agreement or other legal act regulating the relationships with the controller.

5. International Transfers

5.1. If we have the employees, contractors, corporate affiliates, or Data Processors outside of the EEA, and we transfer Personal Data to them for the processing, the Privacy Manager must make sure The Frontend Company takes all necessary and appropriate safeguards in accordance with Data Protection Laws.

5.2. The Privacy Manager must assess the safeguards available and propose to the The Frontend Company's management the appropriate safeguard for each international transfer. The following regimes apply to the transfers of Personal Data outside of the EU:

- where the European Commission decides that the country has an adequate level of personal data protection, the transfer does not require taking additional safeguards. The full list of adequate jurisdictions can be found on the relevant page of the European Commission's website[1].
- to transfer Personal Data to our contractors or partners (Data Processors or Controllers) in other third countries, we must conclude Standard Contractual

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en;

Clauses with that party. The draft version along with the guidance can be found on the relevant page of the European Commission's website[2];
- if we have a corporate affiliate or an entity in other countries, we may choose to adopt Binding Corporate Rules in accordance with Article 47 of the GDPR or an approved code of conduct pursuant to Article 40 of the GDPR;
- we also can transfer Personal Data to entities that have an approved certification in accordance with Article 42 of the GDPR, which certifies an appropriate level of company's data protection.

5.3. As a part of the information obligations, The Frontend Company must inform the Data Subjects that their Personal Data is being transferred to other countries, as well as provide them with the information about the safeguards used for the transfer. The information obligation is to be performed in accordance with Subsection 6.2.

5.4. In the exceptional cases (the "**Derogation**"), where we cannot apply the safeguards mentioned afore and we need to transfer Personal Data, we must take an explicit consent (active statement) from the Data Subject or it must be strictly necessary for the performance of the contract between us and the Data Subject, or other derogation conditions apply in accordance with the Data Protection Laws. The Privacy Manager must pre-approve any Derogation transfers and document the approved Derogations, as well as the rationale for them.

6. Rights of Data Subjects

6.1. **Our Responsibilities**.

6.1.1. Privacy Manager is ultimately responsible for handing all DSR received by The Frontend Company. In the case of receiving any outstanding or unusual DSR, the employee must seek advice from the Privacy Manager before taking any action.

6.1.2. Customer Support within The Frontend Company is responsible for handling DSRs from The Frontend Company Users on a daily basis. The Human Resources department is responsible for handling the DSR from The Frontend Company employees.

6.1.3. All DSRs from the Users must be addressed at and answered from the following e-mail address: info@thefrontendcompany.com. DSR from the employees can be addressed directly to the HR manager or at info@thefrontendcompany.com.

6.1.4. The responsible employee must answer to the DSR within one (1) month from receiving the request. If complying with the DSR takes more than one month in time, the responsible employee must seek advice from the Privacy Manager and, where necessary, inform the Data Subject about the prolongation of the

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en;

response term for up to two (2) additional months.

6.1.5. The responsible employee must analyze the received DSR for the following criteria:

- **Data Subject identification**. Before considering the DSR content, the responsible employee must make sure the Data Subject is the same person he/she claims to be. For this purpose, the connection between the personal data records and the data subject must be established.
  The following methods must be used for this: check of the email address of the Data Subject – generally, the email address should be the same that The Frontend Company has about the user in question; if the email address is different from the record in the database, the Privacy Manager must be consulted, upon the approval of which the responsible employee can request additional details from the account for the identification, such as date of birth, the address, and email address.
  If the Data Subject failed to undergo the verification, the Privacy Manager must refuse to perform the request and inform the Data Subject about it without undue delay, but no later than within one (1) month from receiving the request.
- **Personal data**. The responsible employee must check whether The Frontend Company has access to the personal data requested. If The Frontend Company does not have the personal data under the control, the responsible employee must inform the Data Subject, and, if possible, instruct on the further steps on how to access the data in question;
- **Content of the request**. Depending on the content of the DSR, the responsible employee must define the type of the request and check whether it meets the conditions prescribed by this Policy and Data Protection Laws. The types of requests and the respective conditions for each of them can be consulted in Subsections 6.3-6.9. If the request does not meet the described criteria, the responsible employee must refuse to comply with the DSR and inform the Data Subject about the reasons for refusing;
- **Free of charge.** Generally, all requests of Data Subjects and exercises of their rights are free of charge. If the responsible employee finds that the Data Subject exercises the rights in an excessive or unfound way (e.g., intended to harm or interrupt The Frontend Company's business activities), the employee must seek the advice from the Privacy Manager, and, upon receiving of the latter, may either charge the Data Subject a reasonable fee or refuse to comply with the request;
- **Documenting**. Whenever The Frontend Company receives the DSR, the Privacy Manager must make sure that the data and time, Data Subject, type of the request and the decision made regarding it are well documented. In the case of refusing to comply with the request, the reasons for refusing must be documented as well;
- **Recipients**. When addressing the DSR, the Privacy Manager must make

sure that all concerned recipients were informed the necessary actions were taken.

6.2. **The right to be informed**.

6.2.1. The Frontend Company must notify each Data Subject about the collection and further processing of the Personal Data.

6.2.2. The information to be provided includes: the name and contact details of The Frontend Company; generic purposes of and the lawful basis for the data collection and further processing; categories of Personal Data collected; recipients/categories of recipients; retention periods; information about data subject rights, including the right to complain to the competent Supervisory Authority; the consequences of the cases where the data is necessary for the contract performance and the Data Subject does not provide the required data; details of the safeguards where personal data is transferred outside the EEA; and any third-party source of the personal data, without specification for the particular case (except if we receive the direct request from the Data Subject).

6.2.3. The Users must be informed by the Privacy Policy accessible at The Frontend Company's website and provided during the user registration. The employees and contractors must be informed by a standalone employee privacy statement, which explains the details described in p. 6.2.2 in a case-based manner, describing the particular purposes and activities.

6.2.4. The Frontend Company must inform Data Subjects about data processing, including any new processing activity introduced at The Frontend Company within the following term:

- if personal data is collected from the data subject directly, the data subject must be informed at the time we collect Personal Data from the Data Subjects by showing the Data Subject our privacy statement;
- if the personal data is collected from other sources: (a) within one month from collecting it; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.
- upon the request of the Data Subject; and
- within one (1) month after any change of our personal data practices, change of the controller of Personal Data or after significant changes in our privacy statements.

6.3. **The right to access the information**.

6.3.1. The Data Subject must be provided only with those personal data records specified in the request. If the Data Subject requests access to all personal data concerning her or him, the employee must seek advice from the Privacy Manager first, to make sure all personal data of the Data Subject is mapped and provided.

6.3.2. A Data Subject has the right to:

- learn if we process the Data Subject's Personal Data;

- obtain disclosure regarding aspects of the processing, including detailed and case-specific information on purposes, categories of Personal Data, recipients/categories of recipients, retention periods, information about one's rights, details of the relevant safeguards where personal data is transferred outside the EEA, and any third-party source of the personal data; and
- obtain a copy of the Personal Data undergoing processing upon the request.

6.4. **The right to verify the Data Subject's information and seek its rectification**. The information we collect can be/become inaccurate or out-of-date (e.g., mistakes in nationality, date of birth, info on debts, economic activities). If we reveal that the Personal Data is inaccurate or the Data Subject requests us to do so, we must ensure that we correct all mistakes and update the relevant information.

6.5. **The right to restrict processing**.

6.5.1. The restriction of processing allows Data Subjects to temporarily stop the use of their information to prevent the possible harm caused by such use.

6.5.2. This right applies when the Data Subject:
- contests the accuracy of the Personal Data;
- believes that we process the Personal Data unlawfully; and
- objects against the processing and wants us not to process Personal Data while we are considering the request.

6.5.3. In the case of receiving the restriction request, we must not process Personal Data in question for any other purpose than storing it or for legal compliance purposes until the circumstances of restriction cease to exist.

6.6. **The right to withdraw the consent**. For the activities that require consent, the Data Subject can revoke their consent at any time. If the Data Subject revokes the consent, we must record the changes and must not process the Personal Data for consent-based purposes. The withdrawal of consent does not affect the lawfulness of the processing done before the withdrawal.

6.7. **The right to object against the processing**.

6.7.1. If we process the information in our legitimate interests, e.g., for direct marketing emails or for our marketing research purposes, the Data Subject can object against the processing.

6.7.2. In the case of receiving the objection request case, we must consider Data Subject's request and, where we do not have compelling interests, stop the processing for the specified purposes. If the personal data is still to be processed for other purposes, the Privacy Manager must make sure that the database has a record that the data cannot be further processed for the objected activities.

6.7.3. The objection request can be refused only if the personal data in question is used for scientific/historical research or statistical purposes and was appropriately protected, i.e. by anonymization or pseudonymization techniques.

6.8. **Right to erasure/to be forgotten**.

6.8.1. The Data Subjects have the right to request us to erase their Personal Data if one of the following conditions are met:
- Personal Data is no longer necessary for the purposes of collection. For example, a user has provided personal data for a one-time activity, such as data validation or participation in a contest, and the purpose is already fulfilled;
- the Data Subject revokes one's consent or objects to the processing (where applicable) and there is no other legal ground for the processing; or
- we process the Personal Data unlawfully or its erasure is required by the applicable legislation of the European Union or one of the Member countries of the European Union.

6.8.2. Conditions, under which we have the right to refuse the erasure:
- Personal Data is processed for scientific/historical research or statistical purposes and is appropriately protected, i.e. pseudonymized or anonymized;
- Personal Data is still necessary for legal compliance (e.g., financial or labor laws compliance).

6.8.3. Only those personal data records must be deleted that were specified in the request. If the Data Subject requests the deletion of all personal data concerning her or him, the employee must seek advice from the Privacy Manager first, to make sure all the data about the Data Subject is mapped and can be deleted.

6.8.4. If the User still has an account with us and requests the erasure of information necessary for maintaining the account, we must inform the User that the erasure will affect user experience or can lead to the closure of the account.

6.9. **Data portability**.

6.9.1. Data Subjects can ask us to transfer all the Personal Data and/or its part in a machine-readable format to a third party. This right applies in two cases:
- personal data was collected for the purpose of provision of our services (performance of the contract); or
- collected based on consent.

6.9.2. To determine whether one of the p.6.9.1 conditions are met, the employee must seek advice from the Privacy Manager and check the applicable legal basis in the Records of processing activities. If the answer is negative, the request can be refused by The Frontend Company, and the Privacy Manager must decide whether to comply with the request on a voluntary basis.

6.9.3. To comply with the request, the responsible employee must consolidate requested Personal Data and send the data in the format we are usually

working with to the requested organization. The Data Subject must provide the necessary contact details of the organization.

7. New Data Processing Activities

7.1. **Notification to Privacy Manager**

7.1.1. Before introducing any new activity that involves the processing of personal data, an employee responsible for its implementation must inform the Privacy Manager.

7.1.2. Upon receiving information about a new activity, Privacy Manager must:

- determine whether the data processing impact assessment (DPIA) and/or the consultation with the Supervisory Authority is necessary. If the answer is positive, the Privacy Manager must make sure the DPIA is conducted and/or the Supervisory Authority is consulted in accordance with the requirements of this Section and Data Protection Laws;
- determine the legal basis for the processing and, where necessary, take further action for its fixation;
- make sure the processing activity is done in accordance with this Policy, other The Frontend Company's policies, as well as the Data Protection Laws;
- add the processing activity to the Records of processing activities;
- amend the privacy information statements and, where necessary, inform the concerned Data Subject accordingly.

7.2. **Data Processing Impact Assessment**

7.2.1. To make sure that our current or prospective processing activities do not/will not violate the Data Subjects' rights, The Frontend Company must, where required by Data Protection Laws, conduct the Data Processing Impact Assessment (DPIA), a risk-based assessment of the processing and search for the measures to mitigate the risks. The Privacy Manager must make sure the DPIA is conducted in accordance with this Section.

7.2.2. The Privacy Manager, where necessary, involving the competent employees and/or external advisors, must conduct a DPIA if at least one of the following conditions are met:

- the processing involves the use of new technologies, such as the Artificial Intelligence, use of connected and autonomous devices, etc. that creates certain legal, economic or similar effects to the Data Subject;
- we systematically assess and evaluate personal aspects of the Data Subjects based on automated profiling, assigning the personal score/rate, and create legal or similar effects for the Data Subject by this activity;
- we process on a large scale sensitive data, which includes Personal Data relating to criminal convictions and offences, the data about vulnerable data subjects, the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and

the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

- we collect or process Personal Data from a publicly accessible area or public sources on a large scale, or combine or match two different data sets; and
- the Supervisory Authority in its public list requires conducting a DPIA for a certain type of activity we are involved in. The list of processing activities requiring conducting DPIA can be found on the website of each Supervisory Authority.

7.2.3. The assessment shall contain at least the following details:

- a systematic description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by us. The description must include the envisaged data categories and data subjects concerned, the scale of processing activities, such as its frequency, volume, envisaged number of records, etc.; recipients of the data, retention periods and, where applicable, international transfers;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes. The DPIA must explain whether the activity is necessary for the purpose and whether the purpose can be achieved by less intrusive methods;
- an assessment of the risks to the rights and freedoms of data subjects, including the rights of Data Subjects regarding their Personal Data.
- The examples of risks are the processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects; and
- the measures to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation.

7.2.4. Where the DPIA did not provide how to effectively address the risks, the Privacy Manager must initiate the consultation with the competent Supervisory Authority to receive help with searching for the solution. In this case, The Frontend Company must not conduct the activity before the Supervisory Authority approves the processing activity in question.

8. Data Retention

8.1. **General Rule**.

8.1.1. The Privacy Manager must make sure that The Frontend Company clearly defined the data storage periods and/or criteria for determining the storage periods for each processing activity it has. The periods for each processing activity must be specified in the Records of processing activities.

8.1.2. Each department within The Frontend Company must comply with the data storage periods in accordance with the retention schedule provided in Records of processing activities. The Privacy Manager must supervise each department and make sure they comply with this requirement.

8.1.3. After the storage period ends, the personal data must be removed from the disposal of the department responsible for the processing or, in cases where the data is not needed for any other purposes, destroyed completely, including from back-up copies and other media.

8.1.4. Whenever the storage period for a processing activity has ended, but the personal data processed is necessary for other processing purposes, the department manager must make sure that the personal data is not used for the ceased processing activity, and the responsible employees do not have the access to it unless required for any other activity.

8.2. **Exemptions**. The rules specified in Subsection 8.1 have the following exceptions:

8.2.1. **Business needs**. Data retention periods can be prolonged, but no longer than 60 days, in the case that the data deletion will interrupt or harm our ongoing business. The Privacy Manager must approve any unforeseen prolongation;

8.2.2. **Technical impossibility**. Some information is technically impossible or disproportionally difficult to delete. For example, deletion of the information may lead to breach of system integrity, or it is impossible to delete the information from the backup copies. In such a case, the information can be further stored, subject to the approval by the Privacy Manager and making respective amendments to the Records of processing activities; and

8.2.3. **Anonymization**. The Personal Data can be further processed for any purposes (e.g., marketing) if we fully anonymize these data after the retention period is expired. This means that all personal identifiers and connections to them will be deleted from the data. To consider Personal Data anonymous, it must be impossible to reidentify the Data Subject from the data set.

9. Security

9.1. Each department within The Frontend Company shall take all appropriate technical and organizational measures that protect against unauthorized, unlawful, and/or accidental access, destruction, modification, blocking, copying, distribution, as well as from other illegal actions of unauthorized persons regarding the personal data under their responsibility.

9.2. The employee responsible for the supervision after the security of personal data within The Frontend Company shall be IT specialist. This person implements the guidelines and other specifications on data protection and information security in his area of responsibility. He/she advises The Frontend Company management on the planning and implementation of information security in The Frontend Company, and must be involved in all projects at an early stage in order to take security-related aspects into account as early as the planning phase.

9.3. The detailed list of security measures to comply with is described in our Security Policy.

10. Data Breach Response Procedure

10.1. **Response Team**.

10.1.1. In case of revealing the Data Breach, CEO of The Frontend Company shall urgently form the Data Breach Response Team (the "**Response Team**"), which will handle the Data Breach, notify the appropriate persons, and mitigate its risks.

10.1.2. The Response Team must be a multi-disciplinary group headed by CEO of The Frontend Company and comprised of the Privacy Manager, privacy laws specialist (whether internal or external), and knowledgeable and skilled information security specialists within The Frontend Company or outsourcing professionals, if necessary. The team must ensure that all employees and engaged contractors/processors adhere to this Policy and provide an immediate, effective, and skillful response to any suspected/alleged or actual Data Breach affecting The Frontend Company.

10.1.3. The potential members of the Response Team must be prepared to respond to a Data Breach. The Response Team shall perform all the responsibilities of The Frontend Company mentioned in this Policy. The duties of the Response Team are:

- to communicate the Data Breach to the competent Supervisory Authority(-ies);
- in case of high risk to the rights and freedoms of Data Subjects, to communicate the Data Breach to the Data Subject;
- if The Frontend Company obtain data from any third party as a processor,

and a Data Breach involves obtained data, to inform the third parties about the Data Breach;
- to communicate The Frontend Company's contractors or any other third parties that process the Personal Data involved in the Data Breach; and
- to take all appropriate technical and organizational measures to cease the Data Breach and mitigate its consequences;
- to record the fact of the Data Breach in the Records of processing activities and file an internal data breach report that describes the event.

10.1.4. The Response Team shall perform its duties until all the necessary measures required by this Policy are taken.

10.2. **Notification to Supervisory Authority**.

10.2.1. The Frontend Company shall inform the Competent Supervisory Authority about the Data Breach without undue delay and, where it is possible, not later than 72 hours after having become aware of the Data Breach.

10.2.2. The Competent Supervisory Authority shall be determined by the residence of the Data Subjects, whose information was involved in the Data Breach. If the Data Breach concerns the Personal Data of Data Subjects from more than one country, The Frontend Company shall inform all Competent Supervisory Authorities.

10.2.3. To address the notification to the authority, the Response Team should use Annex 1 to this Policy. Annex 1 contains all the necessary contact information of the EU supervisory authorities. If the Data Breach concerns Data Subjects from other than the EU countries, the Response Team shall ask a competent privacy specialist for advice.

10.2.4. The notification to the Competent Supervisory Authority shall contain, at least, following information:
- **the nature of the Data Breach** including where possible, the categories and an approximate number of Data Subjects and Personal Data records concerned;
- the name and contact details of the **Response Team, Privacy Manager or, if not applicable, of the CEO**;
- the likely consequences of the Data Breach. Explain The Frontend Company's point of view on the purposes and possible further risks of the Data Breach. E.g., the Personal Data may be stolen for the further **sale, fraud activities or blackmailing the concerned Data Subjects**; and
- **the measures taken or proposed** to be taken by The Frontend Company to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.2.5. To file a notification, the Response Team should use The Frontend Company's Data Breach Notification Form to the Supervisory Authority.

10.3. **Notifications to Data Subjects**.

10.3.1. When the Data Breach is likely to result in a high risk to the rights and freedoms

of Data Subjects (e.g., stealing of funds, assets, proprietary information), we must also communicate the Data Breach to the concerned Data Subjects without undue delay. The Privacy Manager must determine if there is a high risk based on the risk factors specified in Subsection 7.2.3 of this Policy.

10.3.2. The notification shall contain the following information:

- description of the Data Breach – what happened and what led to the Data Breach, such as **a security breach, employee's negligence, error in the system work.** If the Response Team decided not to disclose the causes of the Data Breach, then this clause must not be mentioned;
- the measures taken by The Frontend Company regarding the Data Breach, including **security measures, internal investigations, and supervisory authority notice**;
- recommendations for the concerned Data Subjects how to mitigate risks and possible consequences, such as **guidelines on how to restore access to an account, preventing measures (change of a password)**; and
- the contact information of the Response Team or one of its members.

10.3.3. The notification to the Data Subjects should be carried out by the **email letter** or, where it is impossible to use the email, by other available means of communication.

10.3.4. **Exemptions**. We do not have to send the notification to the Data Subjects if any of the following conditions are met:

- The Frontend Company has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Data Breach, in particular, those that leave the Personal Data inaccessible to any person who is not authorized to access it, such as encryption;
- The Frontend Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred to in this section is no longer likely to materialize; or
- it would involve a disproportionate effort to communicate with every concerned Data Subject. 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.

In the case we apply one of the exemptions, we **must document** the circumstances, reason for not informing, and actions taken to meet one of the exemptions.

10.4. **<u>Communication with Third Parties</u>**.

10.4.1. In the case a Data Breach concerns the Personal Data shared with us or processed by us on behalf of a Third Party, we must also notify the Third Party about it within 24 hours. If we process the Personal Data as a Data Processor, the notification of the Third Party does not exempt us from the duty to mitigate the Data Breach consequences, but we must not inform the Competent

Supervisory Authority and Data Subjects.

10.4.2. In case of receiving the notification about the Data Breach from the Data Processor or other Third Parties that have access to the Personal Data, CEO of The Frontend Company shall, in accordance with this Section:

- form the Response Team;
- request the Third Party to send the information mentioned in Subsections 10.2-3 of this Policy;
- where necessary, inform the Competent Supervisory Authority(-ies) and Data Subjects; and
- perform other steps of the Data Breach response procedure.

List of Persons Briefed on Personal Data Protection Policy

№	Full Name	Status	Date	Signature
1.	Oleksandr Vasylenko	Employee		
2.	Viktoria Buchenko	Employee		

ANNEX 1 TO THE PERSONAL DATA PROTECTION POLICY

European National Data Protection Authorities

Austria

Österreichische Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien
Tel. +43 1 531 15 202525
Fax +43 1 531 15 202690
e-mail: dsb@dsb.gv.at
Website: http://www.dsb.gv.at/

Art 29 WP Member: **Dr Andrea JELINEK**, Director, Österreichische Datenschutzbehörde

Belgium

Commission de la protection de la vie privée
Commissie voor de bescherming van de persoonlijke levenssfeer
Rue de la Presse 35 / Drukpersstraat 35 1000 Bruxelles / 1000 Brussel
Tel. +32 2 274 48 00
Fax +32 2 274 48 35
e-mail: commission@privacycommission.be
Website: http://www.privacycommission.be/

Art 29 WP Vice-President: **Willem DEBEUCKELAERE**, President of the Belgian Privacy commission

Bulgaria

Commission for Personal Data Protection
2, Prof. Tsvetan Lazarov blvd. Sofia 1592
Tel. +359 2 915 3580
Fax +359 2 915 3525
e-mail: kzld@cpdp.bg
Website: http://www.cpdp.bg/

Art 29 WP Member: **Mr Ventsislav KARADJOV**, Chairman of the Commission for Personal Data Protection

Art 29 WP Alternate Member: **Ms Mariya MATEVA**

Croatia

Croatian Personal Data Protection Agency
Martićeva 14
10000 Zagreb
Tel. +385 1 4609 000
Fax +385 1 4609 099
e-mail: azop@azop.hr or info@azop.hr
Website: http://www.azop.hr/

Art 29 WP Member: **Mr Anto RAJKOVAČA**, Director of the Croatian Data Protection Agency

Cyprus

Commissioner for Personal Data Protection
1 Iasonos Street,
1082 Nicosia
P.O. Box 23378, CY-1682 Nicosia Tel. +357 22 818 456
Fax +357 22 304 565
e-mail: commissioner@dataprotection.gov.cy
Website: http://www.dataprotection.gov.cy/

Art 29 WP Member: **Ms Irene LOIZIDOU NIKOLAIDOU**

Art 29 WP Alternate Member: **Mr Constantinos GEORGIADES**

Czech Republic

The Office for Personal Data Protection
Urad pro ochranu osobnich udaju Pplk. Sochora 27
170 00 Prague 7
Tel. +420 234 665 111
Fax +420 234 665 444
e-mail: posta@uoou.cz
Website: http://www.uoou.cz/

Art 29 WP Member: **Ms Ivana JANŮ**, President of the Office for Personal Data Protection

Art 29 WP Alternate Member: **Mr Ivan PROCHÁZKA**, Adviser to the President of the Office

Denmark

Datatilsynet
Borgergade 28, 5
1300 Copenhagen K
Tel. +45 33 1932 00
Fax +45 33 19 32 18
e-mail: dt@datatilsynet.dk
Website: http://www.datatilsynet.dk/

Art 29 WP Member: **Ms Cristina Angela GULISANO**, Director, Danish Data Protection Agency (Datatilsynet)

Art 29 WP Alternate Member: **Mr Peter FOGH KNUDSEN**, Head of International Division at the Danish Data Protection Agency (Datatilsynet)

Estonia

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Väike-Ameerika 19
10129 Tallinn
Tel. +372 6274 135
Fax +372 6274 137
e-mail: info@aki.ee
Website: http://www.aki.ee/en

Art 29 WP Member: **Mr Viljar PEEP**, Director General, Estonian Data Protection Inspectorate

Art 29 WP Alternate Member: **Ms Maarja Kirss**

Finland

Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 Helsinki Tel. +358 10 3666 700
Fax +358 10 3666 735
e-mail: tietosuoja@om.fi
Website: http://www.tietosuoja.fi/en/

Art 29 WP Member: **Mr Reijo AARNIO**, Ombudsman of the Finnish Data Protection Authority

Art 29 WP Alternate Member: **Ms Elisa KUMPULA**, Head of Department

France

Commission Nationale de l'Informatique et des Libertés - CNIL
8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02 Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: http://www.cnil.fr/

Art 29 WP Member: **Ms Isabelle FALQUE-PIERROTIN**, President of CNIL

Art 29 WP Alternate Member: **Ms Florence RAYNAL**

Germany

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30
53117 Bonn
Tel. +49 228 997799 0; +49 228 81995 0
Fax +49 228 997799 550; +49 228 81995 550
e-mail: poststelle@bfdi.bund.de
Website: http://www.bfdi.bund.de/

The competence for complaints is split among different data protection supervisory authorities in Germany.
Competent authorities can be identified according to the list provided under https://www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

Art 29 WP Member: **Ms Andrea VOSSHOFF**, Federal Commissioner for Freedom of Information

Art 29 WP Alternate Member: **Prof. Dr. Johannes CASPAR**, representative of the federal states

Greece

Hellenic Data Protection Authority
Kifisias Av. 1-3, PC 11523 Ampelokipi Athens
Tel. +30 210 6475 600
Fax +30 210 6475 628
e-mail: contact@dpa.gr
Website: http://www.dpa.gr/

Art 29 WP Member: **Mr Konstantinos Menoudakos,** President of the Hellenic DPA

Art 29 WP Alternate Member: **Dr.Vasilios ZORKADIS**, Director

Hungary

National Authority for Data Protection and Freedom of Information
Szilágyi Erzsébet fasor 22/C H-1125 Budapest
Tel. +36 1 3911 400
e-mail: peterfalvi.attila@naih.hu
Website: http://www.naih.hu/

Art 29 WP Member: **Dr Attila PÉTERFALVI**, President of the National Authority for Data Protection and Freedom of Information

Art 29 WP Alternate Member: **Mr Endre Győző SZABÓ** Vice-president of the National Authority for Data Protection and Freedom of Information

Ireland

Data Protection Commissioner
Canal House Station Road Portarlington Co. Laois
Lo-Call: 1890 25 22 31
Tel. +353 57 868 4800
Fax +353 57 868 4757
e-mail: info@dataprotection.ie
Website: http://www.dataprotection.ie/

Art 29 WP Member: **Ms Helen DIXON**, Data Protection Commissioner

Art 29 WP Alternate Members: **Mr John O'DWYER**, Deputy Commissioner; **Mr Dale SUNDERLAND**, Deputy Commissioner

Italy

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121 00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
e-mail: garante@garanteprivacy.it
Website: http://www.garanteprivacy.it/

Art 29 WP Member: **Mr Antonello SORO**, President of Garante per la protezione dei dati personali

Art 29 WP Alternate Member: **Ms Giuseppe BUSIA**, Secretary General of Garante per la protezione dei dati personali

Latvia

Data State Inspectorate Director: Ms Daiga Avdejanova
Blaumana str. 11/13-15
1011 Riga
Tel. +371 6722 3131
Fax +371 6722 3556
e-mail: info@dvi.gov.lv
Website: http://www.dvi.gov.lv/

Art 29 WP Alternate Member: **Ms Aiga BALODE**

Lithuania

State Data Protection
Žygimantų str. 11-6a 011042 Vilnius
Tel. + 370 5 279 14 45
Fax +370 5 261 94 94
e-mail: ada@ada.lt
Website: http://www.ada.lt/

Art 29 WP Member: **Mr Raimondas Andrijauskas**, Director of the State Data Protection Inspectorate

Art 29 WP Alternate Member: **Ms Neringa KAKTAVIČIŪTĖ-MICKIENĖ**, Head of Complaints Investigation and International Cooperation Division

Luxembourg

Commission Nationale pour la Protection des Données
1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Tel. +352 2610 60 1
Fax +352 2610 60 29
e-mail: info@cnpd.lu
Website: http://www.cnpd.lu/

Art 29 WP Member: **Ms Tine A. LARSEN**, President of the Commission Nationale pour la Protection des Données

Art 29 WP Alternate Member: **Mr Thierry LALLEMANG**, Commissioner

Malta

Office of the Data Protection Commissioner Data Protection Commissioner: Mr Joseph Ebejer
2, Airways House
High Street, Sliema SLM 1549 Tel. +356 2328 7100
Fax +356 2328 7198
e-mail: commissioner.dataprotection@gov.mt
Website: http://www.dataprotection.gov.mt/

Art 29 WP Member: **Mr Saviour CACHIA**, Information and Data Protection Commissioner

Art 29 WP Alternate Member: **Mr Ian DEGUARA**, Director – Operations and Programme Implementation

Netherlands

Autoriteit Persoonsgegevens
Prins Clauslaan 60
P.O. Box 93374
2509 AJ Den Haag/The Hague Tel. +31 70 888 8500
Fax +31 70 888 8501
e-mail: info@autoriteitpersoonsgegevens.nl
Website: https://autoriteitpersoonsgegevens.nl/nl

Art 29 WP Member: **Mr Aleid WOLFSEN**, Chairman of Autoriteit Persoonsgegevens

Poland

The Bureau of the Inspector General for the Protection of Personal Data - GIODO
ul. Stawki 2
00-193 Warsaw
Tel. +48 22 53 10 440
Fax +48 22 53 10 441
e-mail: kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl
Website: http://www.giodo.gov.pl/

Art 29 WP Member: **Ms Edyta BIELAK-JOMAA**, Inspector General for the Protection of Personal Data

Portugal

Comissão Nacional de Protecção de Dados - CNPD
R. de São. Bento, 148-3° 1200-821 Lisboa
Tel. +351 21 392 84 00
Fax +351 21 397 68 32
e-mail: geral@cnpd.pt
Website: http://www.cnpd.pt/

Art 29 WP Member: **Ms Filipa CALVÃO**, President, Comissão Nacional de Protecção de Dados

Art 29 WP Alternate Member: **Isabel CRUZ**, Secretary-General of the DPA

Romania

The National Supervisory Authority for Personal Data Processing President: Mrs Ancuţa Gianina Opre
B-dul Magheru 28-30
Sector 1, BUCUREŞTI
Tel. +40 21 252 5599
Fax +40 21 252 5757
e-mail: anspdcp@dataprotection.ro
Website: http://www.dataprotection.ro/

Art 29 WP Member: **Ms Ancuţa Gianina OPRE**, President of the National Supervisory Authority for Personal Data Processing

Art 29 WP Alternate Member: **Ms Alina SAVOIU**, Head of the Legal and Communication Department

Slovakia

Office for Personal Data Protection of the Slovak Republic
Hraničná 12
820 07 Bratislava 27
Tel.: + 421 2 32 31 32 14
Fax: + 421 2 32 31 32 34
e-mail: statny.dozor@pdp.gov.sk
Website: http://www.dataprotection.gov.sk/

Art 29 WP Member: **Ms Soňa PŐTHEOVÁ**, President of the Office for Personal Data Protection of the Slovak Republic

Art 29 WP Alternate Member: **Mr Anna VITTEKOVA**, Vice President

Slovenia

Information Commissioner
Ms Mojca Prelesnik Zaloška 59
1000 Ljubljana
Tel. +386 1 230 9730
Fax +386 1 230 9778
e-mail: gp.ip@ip-rs.si
Website: https://www.ip-rs.si/

Art 29 WP Member: **Ms Mojca PRELESNIK**, Information Commissioner of the Republic of Slovenia

Spain

Agencia de Protección de Datos
C/Jorge Juan, 6
28001 Madrid
Tel. +34 91399 6200
Fax +34 91455 5699
e-mail: internacional@agpd.es
Website: https://www.agpd.es/

Art 29 WP Member: **Ms María del Mar España Martí**, Director of the Spanish Data Protection Agency

Art 29 WP Alternate Member: **Mr Rafael GARCIA GOZALO**

Sweden

Datainspektionen
Drottninggatan 29 5th Floor
Box 8114
104 20 Stockholm
Tel. +46 8 657 6100
Fax +46 8 652 8652
e-mail: datainspektionen@datainspektionen.se
Website: http://www.datainspektionen.se/

Art 29 WP Member: **Ms Kristina SVAHN STARRSJÖ**, Director General of the Data Inspection Board

Art 29 WP Alternate Member: **Mr Hans-Olof LINDBLOM**, Chief Legal Adviser

United Kingdom

The Information Commissioner's Office
Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF Tel. +44 1625 545 745
e-mail: international.team@ico.org.uk
Website: https://ico.org.uk

Art 29 WP Member: **Ms Elizabeth DENHAM**, Information Commissioner

Art 29 WP Alternate Member: **Mr Steve WOOD**, Deputy Commissioner

EUROPEAN FREE TRADE AREA (EFTA)

Iceland

Icelandic Data Protection Agency Rauðarárstíg 10
105 Reykjavík
Tel. +354 510 9600; Fax +354 510 9606
e-mail: postur@personuvernd.is

Liechtenstein

Data Protection Office Kirchstrasse 8, P.O. Box 684
9490 Vaduz
Principality of Liechtenstein Tel. +423 236 6090
e-mail: info.dss@llv.li

Norway

Datatilsynet
The Data Inspectorate
P.O. Box 8177 Dep 0034 Oslo
Tel. +47 22 39 69 00; Fax +47 22 42 23 50
e-mail: postkasse@datatilsynet.no

Data Protection Authority: **Mr Bjørn Erik THORN**

Switzerland

Data Protection and Information Commissioner of Switzerland Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter **Mr Adrian Lobsiger**
Feldeggweg 1
3003 Bern
Tel. +41 58 462 43 95; Fax +41 58 462 99 96 e-mail: contact20@edoeb.admin.ch