Document:
PROTECTED

ILPEA

PERSONAL DATA PROTECTION POLICY

Ilpea Sp. z o.o.

Ilpea Group is a leading international manufacturer and supplier of plastic, magnetic and rubber components, primarily for white goods, and the automotive and construction sectors.

Each Ilpea plant has its own unique context, operates in its own environment, in accordance with applicable legal requirements and locally assesses contextual factors that may affect or are affected by the organisation

POLICY APPROVED BY THE PRESIDENT OF THE MANAGEMENT BOARD ON 26 JUNE 2024

1. Definitions

1.1. Controller - Ilpea Sp. z o.o. with its registered office in Chełstówek 2a, 56-416 Twardogóra

1.2. Personal Data - information about a natural person identified or identifiable by one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity, including an image, a voice recording, contact details, location data, information contained in correspondence, information collected through recording equipment or other similar technology.

1.3. Data Protection Officer (DPO) - a person appointed by the Controller to oversee compliance with the Personal Data protection regulations in the Controller's organisation, performing the tasks set out in Article 39 of the GDPR.

or

Personal Data Protection Coordinator (PDPC) - a person appointed by the Controller who performs tasks within the Controller's organisation related to ensuring that the processing of Personal Data complies with applicable law.

1.4. Supervisory Authority - the President of the Personal Data Protection Office or, alternatively, the competent supervisory authority for Personal Data designated by another Member State of the European Union.

1.5. Data Subject - the natural person to whom the Personal Data processed by the Controller relates.

1.6. Policy - this Personal Data Protection Policy.

1.7. Employee - an individual hired by the Controller under an employment contract.

1.8. GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 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.

1.9. Cooperator - the natural person rendering services to the Controller on the basis of a civil law contract (e.g. contract of mandate, contract for specific work).

2. General principles

2.1. This Policy constitutes the basic document governing the Controller's processing of Personal Data.

2.2. The implementation of the Policy is intended to ensure that the Controller's processing of Personal Data complies with the GDPR, regardless of the form (electronic or printed) in which such processing takes place.

2.3. In connection with its activities, the Controller collects and processes Personal Data in accordance with the relevant legislation, including in particular the GDPR, and the processing principle provided for therein, i.e.:

2.3.1. the Controller shall ensure that its processing of Personal Data is lawful and based on one of the grounds for processing set out in the GDPR, i.e. either Article 6(1), Article 9(2) or Article 10 (principle of lawfulness);

2.3.2. the Controller shall ensure that Personal Data is processed in a fair and transparent manner, and in particular it shall always provide information about the processing of Personal Data at the time of collection, including the purpose and legal basis of processing (principle of fairness and transparency);

2.3.3. the Controller shall ensure that Personal Data is collected for specified, explicit and legitimate purposes and is not further processed in a manner incompatible with those purposes (principle of purpose limitation);

2.3.4. the Controller shall ensure that it processes data only to the extent necessary to fulfil the purpose for which the Personal Data was collected (principle of minimisation);

2.3.5. the Controller shall ensure that the Personal Data it processes is correct and, where necessary, updated, and that it shall take all reasonable steps to ensure that Personal Data which is inaccurate in the light of purposes for which it is processed is erased or rectified without delay (principle of accuracy);

2.3.6. the Controller shall ensure that Personal Data is only processed for as long as it is necessary to fulfil the purposes of processing (principle of temporal limitation);

2.3.7. the Controller shall ensure the security of Personal Data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, by implementing appropriate technical or organisational measures (principle of integrity and confidentiality).

2.4. Through appropriate technical and organisational measures the Controller shall ensure that it is possible to demonstrate compliance of the processing of Personal Data with the GDPR and other regulations concerning Personal Data (accountability).

2.5. The Controller shall ensure that all Employees and Associates of the Controller comply with the Policy.

3. Organisation of the Personal Data protection system

3.1. Prior to granting access to the processing of Personal Data, the Controller shall familiarise each Employee, Associate or other persons processing Personal Data under their authority with the Policy, including the procedures and rules relating to the protection of Personal Data in force in the Controller's organisation.

3.2. Processing of Personal Data by Employees and Associates may only be carried out on the basis of the Controller's documented authorisation. In addition, the Controller shall require the authorised persons to maintain the confidentiality of Personal Data and information relating to the security of Personal Data, and to comply with the Policy, including the procedures and rules relating to the protection of Personal Data in force in the Controller's organisation.

3.3. No DPO/PDPC has been appointed.

3.6. Employees and Associates processing Personal Data shall be obliged in particular to:

3.6.1. process Personal Data in accordance with their authorisation and with due diligence;

3.6.2. in the event of observing an incident that may constitute a breach of protection of Personal Data, report it to their immediate superior and to the Director of Human Resources without delay, in accordance with the principles set out in a separate procedure/instruction.

3.6.3. participate in organised Personal Data protection training courses;

3.6.4. maintain the confidentiality of Personal Data and information on how it is secured, in accordance with the signed non-disclosure clause.

4. Security of Personal Data

4.1. The Controller shall implement appropriate technical and organisational measures to ensure a degree of security appropriate to the risk of violation of the rights or freedoms of natural persons of varying probability and seriousness. In doing so, the Controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing.

4.2. When assessing the appropriateness of security level the organisation takes into account in particular the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.3. To ensure the integrity and confidentiality of Personal Data, the Controller shall provide access to Personal Data only to authorised persons and only to the extent that this is necessary in view of the tasks they perform. The Controller shall apply organisational and technical solutions to ensure that all operations concerning Personal Data are recorded and carried out only by authorised persons.

4.4. The Controller shall conduct an ongoing analysis of the risks associated with the processing of Personal Data and monitor the adequacy of the safeguards applied to Personal Data in relation to the identified risks. Where necessary, the Controller shall implement additional measures to enhance the security of Personal Data.

4.5. Where a given type of processing – in particular using new technologies - is, by its nature, scope, context and purposes, likely to result in a high risk of infringement of rights or freedoms of natural persons, the Controller shall assess the effects of the planned processing operations on the protection of Personal Data before processing. If the impact assessment indicates that the processing would result in a high risk if the Controller did not take measures to minimise that risk, the Controller shall consult the Supervisory Authority before commencing processing.

4.6. If the purposes for which the Controller processes Personal Data do not require the Controller to identify the Data Subject, the Controller shall not be required to retain, obtain or process additional information to identify the Data Subject solely to comply with the requirements of the GDPR.

5. Personal Data protection breach

5.1. The Controller shall ensure that Personal Data breaches are reported to the Supervisory Authority, unless the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons. To this end, the Controller shall in particular oblige all persons processing Personal Data to immediately report any perceived breach of protection of Personal Data.

5.2. The Controller shall ensure that it notifies Data Subjects of a Personal Data breach without undue delay if it is likely to result in a high risk of infringement of rights or freedoms.

5.3. In any event, the Controller shall investigate the breach and implement appropriate organisational and technical corrective measures.

5.4. The Controller shall document any breach of protection of Personal Data, including the circumstances of the breach of protection of Personal Data, its consequences and the remedial action taken.

6. Exercise of Data Subjects' rights

6.1. The Controller shall ensure that it exercises the Data Subjects' rights in accordance with the principles set out in the GDPR, including:

6.1.1. the right to information about data processing - the Controller shall provide the person submitting the request with information about the processing of Personal Data, including, in particular, the purposes and legal basis of the processing, the scope of Personal Data held, the entities to which it is disclosed, and the planned date of erasure of Personal Data;

6.1.2. the right to obtain a copy of data - the Controller shall provide the person submitting the request with a copy of the Personal Data concerning them;

6.1.3. the right to rectify data - the Controller shall, upon request, rectify any inconsistencies or errors in processed Personal Data and complete it if incomplete;

6.1.4. the right to data erasure - upon request, the Controller shall erase or anonymise Personal Data whose processing is no longer necessary for any of the purposes for which it was collected;

6.1.5. the right to restrict processing - the Controller shall, upon request, cease performing operations on Personal Data, with the exception of operations to which the Data Subject has consented and its retention, in accordance with the adopted retention rules or until the reasons for restricting the processing of Personal Data cease to exist (e.g. a decision of the Supervisory Authority authorising further processing is issued);

6.1.6. the right to data portability - to the extent that Personal Data is processed by automated means in connection with a contract or granted consent, the Controller shall, upon request, release Personal Data provided by the Data Subject in a computer-readable format;

6.1.7. the right to object to processing for marketing purposes - the Data Subject may object at any time to the processing of Personal Data for marketing purposes, without having to justify such objection;

6.1.8. the right to object to other purposes of processing - the Data Subject may object at any time to the processing of Personal Data that is carried out on the basis of a legitimate interest of the Controller on grounds relating to their particular situation;

6.1.9. the right to withdraw consent - if the Personal Data is processed on the basis of granted consent, the Data Subject has the right to withdraw it at any time, which, however, shall not affect the lawfulness of processing carried out before withdrawal.

7. Contacts with the Data Subject

7.1. The Controller shall implement appropriate measures so that communications with the Data Subject are made in clear, plain language and in a concise, clear and easily accessible form.

7.2. The Controller shall provide information to Data Subjects in writing or by other means, including electronically where appropriate. If the Data Subject so requests, the Controller shall provide the information verbally, provided that it is possible to confirm the Data Subject's identity using other methods.

7.3. The Controller shall facilitate Data Subjects' exercise of their rights under the GDPR, including the rights provided for in Articles 15 to 22 of the GDPR.

7.4. The Controller shall provide information to Data Subjects on the actions taken in relation to a request submitted pursuant to Articles 15 to 22 of the GDPR without undue delay.

8. Personal Data disclosure and outsourcing

8.1. The Controller shall only disclose Personal Data ti another controller if one of the conditions referred to in either Article 6(1) or Article 9(2) of the GDPR is fulfilled.

8.2. The Controller's outsourcing of processing of Personal Data shall be based on a data processing outsourcing agreement or other legal instrument as referred to in Article 28 of the GDPR.

8.3. The outsourcing of processing of Personal Data by the Controller shall take place after prior verification that the processor provides sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR and protects the rights of the Data Subjects. Moreover, the Controller shall take all necessary measures to ensure that its subcontractors and other cooperating entities guarantee the application of appropriate security measures whenever they process Personal Data on behalf of the Controller.

9. Transfer of Personal Data to third countries

9.1. The level of protection of Personal Data outside the European Economic Area (EEA) differs from that provided by European law. For this reason, the Controller shall transfer Personal Data to a third country only when necessary and with an adequate degree of protection ensured, primarily by:

9.1.1. cooperation with processors of Personal Data in countries for which a relevant decision of the European Commission has been issued as to whether an adequate level of protection of Personal Data is ensured;

9.1.2. use of standard contractual clauses issued by the European Commission.

10. Ensuring continuity of compliance

10.1. The Controller shall ensure that the organisation's operations are continuously maintained in compliance with the Personal Data protection requirements of the GDPR, including reviewing and optimising the records and procedures implemented in the organisation.

10.2. To this end, the Controller, among other things, shall monitor changes in legislation, guidelines of national and international data protection authorities and case law of courts and tribunals, and shall take into account best market practices.

11. Appendices

11.1. The Controller shall maintain and apply the following registers and procedures regarding the protection of Personal Data which constitute an integral part of the Policy:

11.1.1. Register of personal data processing authorisations (confidential document)

11.1.2. Register of data processing activities

11.1.3. Register of data processing categories

11.1.4. Procedure 45-IP36 Procedures for personal data protection breaches

12. Final provisions

12.1. The Policy comes into force on the date of signature, i.e. 26/06/2024.

APPROVED

Dr. Ing. LUCA FABIO LUGLI