

PERSONAL DATA PROCESSING POLICY

1. DEFINITIONS

- 1.1. **Controller** – Carrefour Polska Sp. z o.o. located in Warsaw, Targowa 72, 03-734, entered into the Register of Entrepreneurs kept by the District Court for the Capital City of Warsaw in Warsaw, XIII Commercial Division of the National Court Register under the National Court Register Number (KRS): 0000020710, Tax Identification Number (NIP): 9370008168, National Business Registry Number (REGON): 070569406, share capital amounting to 1,970,719,050 PLN.
- 1.2. **Personal Data** – any information relating to an identified or identifiable natural person through one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, including image, voice recording, contact details, location data, information contained in correspondence, information collected via recording equipment or other similar technology.
- 1.3. **Policy** – this Policy of processing Personal Data.
- 1.4. **GDPR** – Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 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.
- 1.5. **Data Subject** – any natural person whose personal data is processed by the Controller, e.g. person visiting the Controller's premises or sending a query to the Controller in the form of an e-mail.

2. PROCESSING DATA BY THE CONTROLLER

- 2.1. In connection with its business activity, the Controller collects and processes Personal Data in accordance with the appropriate provisions of law, including in particular GDPR and data processing rules specified in them.
- 2.2. Controller ensures transparency of data processing, in particular, it always informs about data processing at the time of their collection, including about the purpose and legal basis of processing - e.g. when concluding an agreement for the sale of goods and services. Controller makes sure that data is collected only to the extent necessary for the indicated purpose and processed only for as long as it is necessary.
- 2.3. Processing data, the Controller ensures its safety and confidentiality as well as access to the information on processing for data subjects. If, despite the security measures applied, there has been a breach of the protection of personal data (e.g. "leak" or loss of data), the Controller will inform about such event data subjects in a manner consistent with the provisions.

3. CONTACT WITH THE CONTROLLER

- 3.1. Contact with the Controller is possible via e-mail address at carrefour@galluppolska.pl, telephone number at +48 801 200 000 or in writing at the address of controller's registered office.

- 3.2. Controller appointed the Inspector for the Protection of Personal Data who you can contact via e-mail at iod@carrefour.pl or in writing the address of the controller's registered office in all cases related to the processing of personal data.

4. SECURITY OF PERSONAL DATA

- 4.1. In order to ensure the integrity and confidentiality of data, the Controller implemented procedures allowing access to personal data only to authorised people and only in the scope necessary due to the tasks performed by them. Controller applies organisational and technical solutions in order to ensure that all operations on personal data are registered and performed only by authorised people.
- 4.2. Moreover, the Controller take all necessary actions so that also its contractors and other collaborating entities provide guarantee of using appropriate security measures in any cases of processing personal data at the request of the Controller.
- 4.3. Controller carries out risk analysis on an on-going basis and monitors the adequacy of data security measures applied to the identified threats. In necessary, the Controller implements additional measures to increase data security.

5. OBJECTIVES AND LEGAL GROUNDS FOR PROCESSING

E-MAIL AND TRADITIONAL CORRESPONDENCE

- 5.1. In the case when the Controller sends via traditional or electronic mail correspondence not related to the services provided to the sender or any other agreement concluded with them, personal data included in this correspondence is processed only for the purpose of communication and resolution of the matter addressed by the correspondence.
- 5.2. Legal grounds for processing is the legitimate interest of the Controller (Art. 6 section 1 subsection f of GDPR) consisting in carrying out correspondence addressed to it in connection with its economic activity.
- 5.3. Controller processed only the personal data relevant to the matter addressed by the correspondence. All correspondence is stored in a manner ensuring security of personal data included in it (and any other information) and is disclosed only to authorised people.

TELEPHONE CONTACT

- 5.4. In the case of contacting the Controller by phone, in matters not related to the concluded agreement or provided services, the Controller may request providing personal data only when it is necessary to handle the matter to which the contact relates. Legal grounds in such case is the legitimate interest of the Controller (Art. 6 section 1 subsection f of GDPR) consisting in the necessity of resolving the reported matter related to its economic activity.
- 5.5. Telephone calls can be also recorded - in such case, at the beginning of the conversation appropriate information must be provided. Calls are registered in order to monitor the quality of service provided and verification of the consultants' work, and for statistical purposes. The recordings are available only for the employees of the Controller or people working at the Controller's helpline.
- 5.6. Personal data in the form of conversation recording is processed:

- 5.6.1. for purposes related to customer service via helpline, if the Controller provides such service - legal grounds for processing is the necessity of processing to provide services (Art. 6 section 1 subsection b of GDPR);
- 5.6.2. to monitor the quality of service and verify the work of consultants working at the helpline, as well as for analytical and statistical purposes - legal basis for the processing is the legitimate interest of the Controller (art. 6 section 1 subsection f of GDPR) consisting in taking care of the highest quality of customer service and consultants work as well as carrying out statistical analyses concerning telephone communication.

VIDEO MONITORING AND ACCESS CONTROL

- 5.7. In order to ensure the safety of people and property, the Controller uses video monitoring and controls the access to the premises and area it manages. Data collected in this way is not used for any other purposes.
- 5.8. Personal data in the form of recordings from monitoring and data collected in the entry and exit register is processed in order to ensure security and order on the premises and possibly for the protection against claims or pursuing these claims. Legal grounds for processing personal data is the legitimate interest of the Controller (Art. 6 section 1 subsection f of GDPR) consisting in ensuring security of the Controllers property and protection of its rights.

RECRUITMENT

- 5.9. Within recruitment processes, the Controller expects providing personal data (e.g. in a CV or resume) only in the scope specified in the Labour Law. Therefore, information of the wider extend should not be transferred. In the case when the applications sent include some additional data, it will not be used and taken into consideration in the recruitment process.
- 5.10. Personal data is processed:
 - 5.10.1. in order to comply with legal obligations resulting from the provisions of law, related to the employment process, including in particular the Labour Code - legal grounds for processing is the legal duty of the Controller (Art. 6 section 1 subsection c of GDPR in relation to the provisions of the Labour Code);
 - 5.10.2. in order to carry out the recruitment process in the scope of data not required by the provisions of law, and for the purpose of the future recruitment processes - legal grounds for processing is consent (art. 6 section 1 subsection a of GDPR);
 - 5.10.3. in order to determine or pursue the possible claims or defence against such claims - legal grounds for such data processing is the Controller legitimate interest (Art. 6 section 1 subsection f of GDPR).

COLLECTING DATA IN CONNECTION WITH THE PROVISION OF SERVICES OR EXECUTION OF OTHER AGREEMENTS

- 5.11. In the case of collecting data for the purposes related to the execution of a specific agreement, the Controller provides the data subject with information concerning the processing of its personal data at the time of the conclusion of the agreement.

COLLECTING DATA IN OTHER CASES

- 5.12.** In connection with the conducted activity, the Collector collects personal data also in other cases - e.g. during business meetings, at industry events or through exchange of business cards - for the purposes related to initiating and maintaining business contacts. Legal grounds in such case are the legitimate interest of the Controller (Art. 6 section 1 subsection f of GDPR) consisting in creating the network of contacts in connection with the conducted activity.
- 5.13.** Personal data collected in such cases is processed only in the purpose for which it was collected, and the Controller ensures its protection.

6. DATA RECIPIENT

- 6.1.** In relation to conducting activity requiring processing, data is disclosed the external entities, including in particular providers responsible for handling IT systems and equipment (e.g. CCTV equipment), entities providing legal or accounting services, deliverymen, marketing or recruitment agencies.
- 6.2.** Controller reserves the right to disclose selected information concerning a data subject to the competent authorities or third parties that request providing such information, based on an appropriate legal grounds and in accordance with the applicable provisions of law.

7. TRANSFERRING DATA OUTSIDE EEA

- 7.1.** The level of protection of personal data outside the European Economic Area (EEA) differs from the one provided by European law. For this reason the Controller transfers personal data outside EEA only when it is necessary, and ensuring at the same time the appropriate level of protection, primarily through:
- 7.1.1.** cooperation with entities processing personal data in countries, in relation to which an appropriate decision of the European Commission was issued;
 - 7.1.2.** use of standard contractual clauses issued by the European Commission;
 - 7.1.3.** use of binding corporate rules approved by the competent supervisory authority;
 - 7.1.4.** in the case of transferring data to the US - cooperation with entities participating in the Privacy Shield program, approved by the decision of the European Commission.
- 7.2.** Controller always informs about the intention of transferring personal data outside EEA at the collection stage.

8. PERIOD OF PROCESSING PERSONAL DATA

- 8.1.** The period of processing data by the Controller depends on the type of service provided and the purpose of processing. The period of processing data can also result from the provisions of law when they constitute legal grounds for processing. In the case of processing data based on the legitimate interest of the Controller - e.g. due to security reasons - data is processed for a period of time allowing the realisation of this interest or the submission of effective opposition against data processing. If the processing is performed based on the consent, data is processed until the consent is withdrawn. When the grounds for processing

are the necessity for the conclusion and the execution of the agreement, data is processed till the date of its resolution.

- 8.2. The data processing period can be extended in the case when processing is necessary to determine or pursue claims or defence against claims, and after this period - only in the case and in the scope in which it will be required by the provisions of law. After the period of processing ends, data is irreversibly deleted or anonymised.

9. RIGHTS RELATED TO THE PROCESSING OF PERSONAL DATA

RIGHTS OF DATA SUBJECTS

- 9.1. Data subjects are entitled to the following rights:

- 9.1.1. **right to information about the processing of personal data** – on this basis the person submitting request is informed by the Controller about the processing of personal data, including about all purposes and legal grounds of processing, scope of possessed data, entities to which it is disclosed and planned date of its deletion;
- 9.1.2. **right to obtain a copy of data** – on this basis the Controller transfers a copy of the processed data relating to a person submitting the request;
- 9.1.3. **right to rectify** – Controller is obliged to delete possible discrepancies or errors in the processed personal data and complete it if it is incomplete;
- 9.1.4. **right to erasure** – on this basis it is possible to erase data the processing of which is no longer necessary to realise any of the objectives for which it was collected;
- 9.1.5. **right to restrict processing** – in the case of submitting such request, the Controller ceases to perform operations on personal data - except for operations agreed by the data subject - and store it, in accordance with accepted retention rules or until the reasons for restricting data processing cease to exist (e.g. a decision of a supervisory authority allowing further processing is issued);
- 9.1.6. **right to data portability** – on this basis - in the scope in which data is processed in connection with the concluded agreement or consent given - the Controller issues data provided by the data subject, in the format allowing them to be read by the computer. It is possible also to request the data to be sent to another entity - provided, however, that there are technical possibilities in this regard on the part of the Controller as well as the other entity;
- 9.1.7. **right to object to the processing of data for marketing purposes** – data subject can at any time object to the processing of data for marketing purposes, without the need to justify such objection;
- 9.1.8. **right to object to other purposes of data processing** – data subject can at any time object the processing of personal data performed based on the legitimate interest of the Controller (e.g. for analytical or statistical purposes or due to the reasons connected to the property protection); objection in this regard should include justification;
- 9.1.9. **right to withdraw consent** – if data is processed based on the expressed consent, the data subject has right to withdraw it at any time, which, however, does not affect the lawfulness of processing performed prior to the withdrawal of the consent.

- 9.1.10. right to complaint** – if it is decided that the processing of personal data violates the provisions of GDPR or any other provisions related to the protection of personal data, the data subject can submit a complaint to the President of the Office of Personal Data Protection.

SUBMITTING REQUESTS RELATED TO THE EXECUTION OF RIGHTS

- 9.2.** Application concerning the exercise of rights of data subjects can be submitted:
- 9.2.1.** in writing to the following address: Carrefour Polska Sp. z o.o., Targowa 72, 03-734 Warsaw,
 - 9.2.2.** by e-mail to the following address: carrefour@galluppolska.pl.
- 9.3.** If the Controller is unable to identify a person submitting application based on the submitted application, it will ask the application for further information.
- 9.4.** The application can be submitted in person or through a proxy (e.g. a family member). For the reasons of data security, the Controller encourages the use of a power of attorney in the form certified by a notary public or an authorised legal advisor or attorney, which will significantly accelerate the verification of application authenticity.
- 9.5.** The response for the application should be given within one month from its submission. In the case when it is necessary to extend this time limit, the Controller informs the applicant about the reasons for the delay.
- 9.6.** The response is given via traditional mail, unless the application was submitted via e-mail or a response in electronic form was requested.

PRINCIPLES OF CHARGING FEES

- 9.7.** Proceedings regarding the submitted applications are free of charge. The fees can be charged only in the following cases:
- 9.7.1.** request for issuing a second and each subsequent copy of data (first copy of data is free of charge); in such case the Controller can request a payment of 50 PLN.

The above-mentioned fee includes administrative costs related to the realisation of the request.
 - 9.7.2.** submitting by the same person excessive demands (e.g. extremely frequent) or clearly unjustified; in such case the Controller can demand the payment of 50 PLN.

The above-mentioned fee included the costs of communication and the costs associated with taking the required actions.
- 9.8.** In the case when the decision about charging fee is questioned, the data subject can submit a complaint to the President of the Office of Personal Data Protection.

10. AMENDMENTS TO THE PERSONAL DATA PROCESSING POLICY

- 10.1.** The policy is verified on an ongoing basis and updated if necessary. The current version of the Policy was adopted on 11 May 2018.