

# Partner in Pet Food Hungária Kft. Data Protection Notice

Latest update: 25 April 2022



## **List of Contents**

1.	GENERAL INFORMATION .....	3
2.	UPDATES AND AVAILABILITY .....	3
3.	SPECIFIC DATA PROTECTION TERMS.....	3
4.	SCOPE OF THE DATA AND THE PURPOSE OF ITS PROCESSING .....	4
5.	DATA PROCESSORS.....	18
6.	TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES .....	21
7.	DATA PROTECTION RIGHTS AND REMEDIES .....	21

## 1. GENERAL INFORMATION

**Partner in Pet Food Hungária Korlátolt Felelősségű Társaság (“Company”)** processes information in connection with third parties, contact persons of its business partners that work with the Company and other individuals, such as consumers (collectively: “**individuals**”). This information qualifies as “*personal data*” as defined in point 1 of Article 4 of the General Data Protection Regulation 2016/679 of the EU (“**GDPR**”).

This data protection notice (“**Notice**”) provides information regarding the processing of this personal data and the rights and remedies of the individuals with regards to said data processing.

### **Contact details of the Company:**

The registered seat of the Company: H-2040 Budaörs, Puskás Tivadar utca 14 The registration number of the Company: Cg. 13-09-090774

The Company is registered at the Company Court of the Tribunal of the Budapest Region

The telephone number of the Company: +36 1 801 02 03

The e-mail address of the Company: info@ppfeurope.com

The website of the Company: <http://www.ppfeurope.com/>

Data Privacy Responsible for the Company and his / her contact details: [dataprivacy@ppfeurope.com](mailto:dataprivacy@ppfeurope.com)

## 2. UPDATES AND AVAILABILITY

The Company reserves the right to unilaterally modify this Notice with immediate effect subsequent to such modification, subject to the limitations provided for by law and the requirements of advance notification to the individuals in due time, if necessary. The Company may modify this Notice, particularly when it is required as a result of changes in the laws, the practice of the data protection authority, business needs or employees’ needs, any new activity involving personal data processing or any newly revealed security exposures, or if it is deemed necessary because of individuals’ feedback. When communicating in relation to this Notice or privacy issues, or otherwise keeping in contact with individuals, the Company may use the contact details of individuals available to the Company in order to get or keep in contact with individuals. Upon the request of an individual, the Company will, for example, send a copy of the latest updated version of this Notice to individuals or certify that a certain individual has read the Notice.

## 3. SPECIFIC DATA PROTECTION TERMS

In certain cases, specific privacy-related terms and conditions may also be applicable to certain individuals; said individuals will be duly notified thereof. Such specific terms and conditions are provided for in connection with the operation of electronic surveillance systems (i.e. cameras), the entry-control systems operated in the offices of the Company, and cookies that are used on the website of the Company.

In each case, individuals are obliged to make the relevant personal data available to the Company in accordance with the applicable laws. Individuals shall especially be in possession of adequate and informed consent, or any other appropriate legal basis, for making personal data available to the Company (for example if the data of contact persons and family members are given). If the Company becomes aware that any personal data of a data subject was disclosed without his/her consent or any other appropriate legal basis, then the Company may immediately delete such personal data, and the data subject is also entitled to exercise the rights and remedies set forth in this Notice. The Company will not be liable for any loss or harm which may arise from any breach of the above undertaking and representation of any individual.

#### 4. **SCOPE OF THE DATA AND THE PURPOSE OF ITS PROCESSING**

The table below describes the scope of the processed personal data, the purposes, the legal basis, the duration of the processing and the scope of the persons authorised to have access to the data. Where a purpose of processing is required for pursuing a legitimate interest of the Company or any third party, then the Company will perform a balancing test of the underlying interests, which is available upon a request submitted to the Company by means of the contact details listed hereinabove.

**The Company expressly wishes to draw the attention of the individuals to their right of objection to the processing of their personal data on grounds relating to their particular situation at any time where the processing is based on a legitimate interest, including cases where the processing takes the form of profiling. In such cases, the Company shall cease to process the personal data unless it can prove that the processing has to be continued due to compelling legitimate reasons which override the interests, rights and freedoms of the individuals, or which relate to the submission, the enforcement or the protection of legal claims. If personal data is processed for the purpose of direct marketing, individuals may at any time object to the processing of their personal data for that purpose. Said grounds for objection include profiling if it is connected to direct marketing.**

Where this Notice indicates the relevant limitation period for the enforcement of claims as the duration of data processing, then any event which interrupts the limitation period shall extend the term of the data processing until the new date when the underlying claim may lapse (Section 6:25 (2) of Act V of 2013 on the Civil Code – the “**Civil Code**”). If the limitation period is interrupted, the claim can be enforced within one year from the time when the reason for interruption ceases to exist or, in respect of a limitation period of one year or less, within three months, even if the limitation period has already lapsed or there is less than one year or less than three months, respectively, remaining from it (Section 6:24 (2) of the Civil Code).

The 8 years’ retention period specified in Act C of 2000 on accounting (the “**Accounting Act**”) shall be counted from the day of a given year when the accounting item related to the data or the accounts/accounting relied on or made use of the relevant data in any way. In practice if the data appears in an agreement under which more completions arise (e.g. advice is provided several times during the term of the agreement), the 8 years’ period shall be counted from each completion separately, because there is a separate invoice for each completion, based on which the transaction is entered into the accounts. If the data appears in an agreement which, for example, provides for the sale and purchase of a single thing (handover takes place and upon completion the agreement terminates), then the transaction is entered into the books under the agreement based on the invoice in the given year and the 8 year retention period starts from then.

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p><b>Allowing participation in promotions and advertising campaigns (including prize games organised by the Company)</b> – in accordance with the applicable terms and conditions of participation</p>	<p>Article 6 (1) (a) of the GDPR – voluntary consent of the individual given in the course of his/her participation in the promotion or advertising campaign in accordance with the applicable terms and conditions of participation.</p> <p><b>The individual may withdraw his/her consent at any time.</b> The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>Without the consent, the individual cannot participate in the given promotion, advertising campaign or prize game.</p>	<p>The scope of participating persons and the personal data are determined on a case-by-case basis, in accordance with the applicable terms and conditions of participation (e.g. name, address and the chosen gift, vote cast in a public voting game open for the public etc.).</p>	<p>The duration of processing is determined on a case-by-case basis, in accordance with the applicable terms and conditions of participation, taking into account the closing date of the promotion or advertising campaign and the time required for the delivery of the prizes, where applicable.</p> <p><b>Authorised persons having access to the data within the Company:</b> determined on a case-by-case basis, in accordance with the applicable terms and conditions of participation, failing which the persons having tasks in relation to the promotion or advertising campaign are authorised to have access to the data.</p>
<p><b>Sending advertisements and newsletters by email</b></p>	<p>Article 6 (1) (a) of the GDPR – voluntary consent of the individual and Section 6 (1) of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities – prior, clear and express consent of the individual.</p> <p><b>Consent may be withdrawn at any time, without limitation and reasoning, free of charge.</b> The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>Without consent, the Company is not permitted to send out advertisements and newsletters by email.</p>	<p>Name and email address of possible recipients.</p>	<p>If an individual withdraws consent, then personal data has to be deleted.</p> <p><b>Authorised persons having access to the data within the Company:</b> persons sending out advertisements and newsletters.</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p><b>Making records of and recordings at Company events</b></p> <p><b>The invitation to the event or information letters placed at the event may give further information about the method of usage of photos and recordings.</b></p>	<p>Article 6 (1) (a) of the GDPR (voluntary consent of the individual).</p> <p><b>The individual may withdraw his/her consent at any time.</b> The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>Without the individual's consent, no photos can be taken and recordings can be made.</p> <p>No consent is needed for taking photos or making recordings and using them where the recordings are made at activities of the individual which qualify as acting in public or where a mass of persons is depicted (Section 2:48 of the Civil Code). In this case the legal basis for making and using recordings is Article 6 (1) (f) of the GDPR (data processing is needed for the legitimate interests pursued by the Company).</p> <p>Legitimate interest: It is the Company's business interest to take photos or make and use recordings to strengthen the image of the Company in business and make the Company better known, give incentive to employees, and improve the atmosphere in the workplace.</p>	<p>Taking photos or making videos at events organised by the Company (images of individuals). With the consent of the individuals or subject to the legitimate interest of the Company (where photos are taken or recordings are made at activities of an individual which qualify as acting in public or where a mass of persons is depicted), the photos or videos may be published in the intranet as well as on external online sites of the Company (e.g. the website, LinkedIn or other social network site of the Company) or on other online or offline media (e.g. online or printed corporate marketing materials).</p>	<p>Photos and recordings may be deleted at any time when the individual so requests. In the case of photos and recordings which have been made public, however, the right of withdrawal can only be exercised fully until the time when such materials appear publicly. For instance, where photos have appeared publicly, third parties might copy and/or save them, which is outside the control of the Company.</p> <p>In respect of printed materials, the Company is not able to withdraw printed copies that have been placed on the market and are no longer within the control of the Company if consent is withdrawn.</p> <p>Individuals give consent in the knowledge of and in acknowledgement of the above restrictions.</p> <p>The Company processes photos and recordings based on its legitimate interest until the relevant individual exercises his/her right of objection.</p> <p><b>Authorised persons having access to the data within the Company:</b> until photos or recordings have not appeared publicly, such recordings are handled by the HR and Marketing Department.</p> <p>Photos and recordings which have been made public on the intranet of the Company, can be seen by all members of the Company's personnel.</p> <p>The materials appearing on the LinkedIn site of the Company and on any online or other media are public.</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p><b>Sending information on the Company's activities – for example, invitations to events organised by the Company, for marketing the Company for non-natural persons (B2B)</b></p>	<p>Article 6 (1) (f) of the GDPR (processing of the data is needed for pursuing the legitimate interests of the Company).</p> <p>The legitimate interest: providing information and marketing on the Company's activities, and successful and efficient organisation of the events of the Company.</p>	<p>Contact details of the persons who are in contact with the Company (e.g. who gave their business cards to the Company or who the Company intends to invite to its events): the names and the organisations they represent and other data they may provide in connection with their participation (e.g. regarding events - anticipated time of arrival, preferred presentation or other event, etc.).</p>	<p>Unless the individual objects to the processing of his/her data, contact details can be used also after the relevant communication or event for the same purposes. The Company stores the data for 5 years after the last contact made with the individual (Section 6:22 (1) of the Civil Code – claims lapse in 5 years).</p> <p><b>Authorised persons having access to the data within the Company:</b> employees of the Marketing Department</p>
<p><b>Processing the personal data of contact persons of contracting partners or potential contracting partners and/or persons involved in the request for a proposal, the submission of a proposal, contract performance / verification of performance (i.e. day-to-day management of proposals or the implementation of contracts).</b> This includes e.g. the processing of postal addresses of relevant persons, their payment instructions or the sending official notifications with the use of the contact details and information regarding</p>	<p>It depends on whether a contact is made or a contract is concluded with the individual (e.g. a private entrepreneur) or with any other undertaking; it is Article 6 (1) (b) of the GDPR – the purpose is directly the performance (implementation) of the contract or taking steps at the request of the individual prior to entering into a contract to which the individual is subject / it is Article 6 (1) (f) of the GDPR – pursuing the legitimate interests of both the Company and the contracting partner: fulfilling the obligations, exercising the contractual rights and business cooperation between the contracting parties.</p> <p>The exchange of personal data is required under the contract; without them, the Company is unable to request a proposal, submit a proposal, conclude the contract and/or implement it.</p>	<p>The contact details (i.e. e-mail addresses, telephone numbers, mobile phone numbers, telefax numbers, description of the relationship with the individual) of the potential contact persons and the actual contact persons of the partners and/or persons involved in the request for a proposal, the submission of a proposal, contract performance and verification of performance, actions related to developing the relationship with the partner and any other activity of or communication which includes any kind of personal data (e.g. communication received from a contact person or any other person acting on behalf of a partner) in connection with the proposal or the contract.</p> <p>The personal data are either provided to the Company by the</p>	<p><b>5 years</b> after the date when the contractual relation ceased (Section 6:22 (1) of the Civil Code – claims lapse in 5 years) or (if this period is different) from the date of the last contact (inactivity) with the contact person. For example, a purchaser may enter an “inactive” status if he or she is transferred to another department at that partner and the Company contacts a new purchaser, or if the contact of that contact terminates at the partner and is replaced by a new contact. It is in the legitimate interest of both the Company and the given partner in this case, that they still know – within the limitation period established by the Civil Code – who the contact's predecessor was and who they can refer to, or they can continue to look for a question where background knowledge of previous transactions is required.</p> <p><b>Tax obligations:</b> data retention period is <b>5 years</b> from the last day of the calendar year in which the tax concerned should have been declared or reported or, in the absence of such declaration or report, the tax should have been paid (Sections 78 (3) and 202 (1) of Act CL of 2017 on the Taxation</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p>proposal-related or contractual obligations to be fulfilled.</p>		<p>partner, or the individuals themselves; and the Company may collect them from publicly available, lawful sources (e.g., partner website, company register).</p>	<p>Procedure –“<b>Taxation Act</b>”).</p> <p><b>Accounting documents:</b> the data retention period is <b>8 years</b> (Sections 168-169 of the Accounting Act. In practice this means when the data are included in documents which support the accountancy records e.g. for example the data appear in contract documents between the Company and the counterparty (such as an order) or on an invoice.</p> <p><b>Authorised persons having access to the data within the Company:</b> areas competent under the contract.</p>
<p><b>Processing the personal data of contact persons of contracting partners and/or persons involved in contract performance and verification of performance in connection with compliance issues or any other activity needed to implement the contract including seeking remedies in order to enforce the rights arising from the contracts</b></p>	<p>The legal basis of processing data is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR). The legitimate interest: handling compliance issues or any other activity needed to implement the contract including seeking remedies in order to enforce the rights arising from the contracts.</p>	<p>The contact details (i.e. e-mail addresses, telephone numbers, mobile phone numbers, telefax numbers) of the contact persons of the contracting partners and/or persons involved in contract performance and verification of performance, and any other activity or communication which includes any kind of personal data (e.g. any communication received from a contact person or any other person acting on behalf of a contracting partner) in connection with the contract.</p> <p>The personal data is provided to the Company either by the contracting partner or the individuals themselves.</p>	<p><b>5 years</b> after the date when the contractual relation ceased (Section 6:22 (1) of the Civil Code – claims lapse in 5 years)</p> <p><b>Tax obligations:</b> duration of data storage is <b>5 years</b> from the last day of the calendar year in which the tax concerned should have been declared or reported or, in the absence of such declaration or report, the tax should have been paid (Sections 78 (3) and 202 (1) of the Taxation Act).</p> <p><b>Accounting documents:</b> duration of data storage is <b>8 years</b> (Sections 168-169 of the Accounting Act). E.g. the data that is included in documents which support the accountancy records e.g. data in contract documents between the Company and the counterparty (such as an order) or on an invoice.</p> <p><b>Authorised persons having access to the data within the Company:</b> areas competent under the contract.</p>



Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p><b>Handling customer and other inquiries received by the Company</b></p>	<p>Article 6 (1) (f) of the GDPR (processing is needed to pursue the legitimate interests of the Company).</p> <p>The legitimate interest: handling customer and other inquiries, responding to inquiries, and the mutual performance of the obligations arising from customer contracts.</p>	<p>The personal data affected by the customer and other inquiries that are received by the Company, the contact data of the customers and other private individuals (i.e. name, address, e-mail address, telephone number) and the records of the actions taken in relation to the inquiry.</p>	<p><b>5 years</b> after responding to an inquiry (Section 6:22 (1) of the Civil Code – claims lapse in 5 years)</p> <p><b>Authorized persons having access to the data within the Company:</b> Customer Service – “CS”.</p> <p>The Company transfers the data within its company group to:</p> <p>Partner in Pet Food Polska SP.z.o.o. ul. Szamocka 8, Warsaw 01-748, Poland telephone No: +48 22 569 24 10, <a href="mailto:info.pl@ppfeurope.com">info.pl@ppfeurope.com</a>.</p> <p>Partner in Pet Food CZ s.r.o. Bucharova 1423/6 158 00 Prague 13 – Nové Butovice, Czech Republic telephone No: +420 234 111 111; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Partner in Pet Food SK s.r.o. Kračanská cesta 40, 929 01 Dunajská Streda, Slovakia telephone No: +421 31 559 13 65; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Partner in Pet Food NL B.V. Wijchenseweg 132 6538 SX Nijmegen, Holland telephone No: +31 24 34 35 910; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Legal basis of the data transfer: Article 6 (1) (f) of the GDPR (the data transfer is needed for pursuing the legitimate interests of the Company and its group companies). The legitimate interest: using</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
			the knowledge of the company group for more efficient processing of customer and other requests and sharing the relevant experience to serve customers better.
<p><b>Handling consumer inquiries received by the Company</b></p> <p>In general consumer inquiries (e.g. questions, comments or complaints) are forwarded to the Company by its contracting partners (e.g. Lidl, Tesco, etc.). The Company may respond to such inquiries directly or assist the contracting partners in responding.</p> <p>If an inquiry is received through social media (e.g. Facebook) then the terms and conditions of the social media service provider for data processing and use may also be applicable.</p>	<p>Article 6 (1) (f) of the GDPR (processing is needed for pursuing the legitimate interests of the Company and those of its contracting partner).</p> <p>The legitimate interest: handling consumer requests is in the legitimate business interest of both the Company and its contracting partner. In addition, handling consumer requests is also a legal requirement for the contractual partner pursuant to article 17/A of the Act CLV of 1997 on consumer protection (“<b>Consumer Protection Act</b>”). The Company provides assistance with this thereby accelerating the process of responding to consumer requests and processing consumer complaints and enhancing the same with the information in its possession.</p>	<p>The personal data affected by consumer inquiries that are received by the Company, contact data of consumers and the contact persons of contracting partners (name, address, e-mail, telephone number), the content of the claims (complaints), inquiries presented by consumers concerned, the records of actions taken, and the contents of the minutes made under Section 17/A of the Consumer Protection Act.</p>	<p><b>5 years</b> after responding to an inquiry (Section 6:22 (1) of the Civil Code – claims lapse in 5 years). The minutes taken on the consumer complaint and the response to it also have to be stored for <b>5 years</b> (Section 17/A (7) of the Consumer Protection Act).</p> <p><b>Authorised persons having access to the data within the Company:</b> Customer Service “CS”.</p> <p>The Company transfers the data within its company group to:</p> <p>Partner in Pet Food Polska SP.z.o.o. ul. Szamocka 8, Warsaw 01-748, Poland telephone No: +48 22 569 24 10, <a href="mailto:info.pl@ppfeurope.com">info.pl@ppfeurope.com</a>.</p> <p>Partner in Pet Food CZ s.r.o. Bucharova 1423/6 158 00 Prague 13 – Nové Butovice, Czech Republic telephone No: +420 234 111 111; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Partner in Pet Food SK s.r.o. Kračanská cesta 40, 929 01 Dunajská Streda, Slovakia telephone No: +421 31 559 13 65; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Partner in Pet Food NL B.V. Wijchenseweg 132 6538 SX Nijmegen, Holland</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
			<p>telephone No: +31 24 34 35 910;  <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p>Legal basis of the data transfer: Article 6 (1) (f) of the GDPR (the data transfer is needed for pursuing the legitimate interests of the Company and its group companies). The legitimate interest: use of the knowledge of the company group for more efficient processing of consumer inquiries and sharing the relevant experience to serve consumers better.</p>
<p><b>Handling data of visitors arriving by vehicle for Company property security purposes</b></p>	<p>Article 6 (1) (f) of the GDPR (processing is needed for pursuing the legitimate interests of the Company).</p> <p>Legitimate interest: the protection of the Company's property and territory, monitoring of products and shipments to and from the premises of the Company and vehicle traffic.</p>	<p>Regarding the visits, the competent staff of the security department record the license-plate numbers of the vehicles driven and the telephone numbers (mobile numbers) indicated by the drivers concerned in the personnel and vehicle logbook.</p>	<p><b>Data retention period: 1 year</b> after the date of the visit (for reasons associated with security of property, monitoring products and shipments to and from the Company's premises and organisation of vehicle traffic).</p> <p><b>Authorised persons having access to the data within the Company:</b> employees of the security service department, central shipment organisation area, and the competent employees of warehouse.</p> <p><b>Humannestor Kft.</b> (registered seat: 7187 Bonyhád-Majos, V. u. 71.), which is in charge of the security surveillance of the Company's premises, also has access to the data.</p>
<p><b>Transport organisation by using the Transporeon system.</b></p>	<p>Article 6 (1) (f) of the GDPR (data processing is necessary to enforce the legitimate interests of the Company).</p> <p>The legitimate interest is to optimise the Company's logistics procedures.</p>	<p>Data relating to transport orders: data relating to transport (loading, exact place, address, date of unloading, etc.), offers, transport documents, etc., as well as the driver's name and telephone number, registration number of the means of transport carrying the transport (for contact with the</p>	<p>Data retention period: 3 months.</p> <p>In the course of data processing, the Company uses the services of TRANSPOREON GmbH, which acts as an independent data controller, as described in its own data protection notice. Contact information for TRANSPOREON GmbH: <a href="http://www.transporeon-group.com">www.transporeon-group.com</a>, <a href="mailto:info@transporeon.com">info@transporeon.com</a>, +1 267-281-1555,</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
		driver), comments on freight.	Magirus-Deutz-Straße 16, 89077 Ulm, Germany.  Transporeon's data protection notice is available at <a href="https://legal.transporeon.com/DP/PLT/en_Platform_Privacy_Policy.pdf">https://legal.transporeon.com/DP/PLT/en_Platform_Privacy_Policy.pdf</a>
<p><b>Register of visitors and entry statement regarding the visitors of PPF's premises.</b></p> <p>This includes handling visitors' data and the entry statements collected from visitors of the premises of the plant, which contains questions regarding health status of visitors for medical, hygienic and production safety reasons.</p>	<p>Article 6 (1) (f) of the GDPR (processing is needed for pursuing the legitimate interests of the Company and its contracting partners).</p> <p>Legitimate interest: Compliance with the medical, hygienic and production regulations, producing products that are safe and not hazardous for health, protecting the health of the animals, protection of the Company's financial interests and confidential information.</p> <p>As regards the processing of medical data: Article 9 (2) (g) of the GDPR (processing is necessary for reasons of substantial public interest - in particular the health of animals, and producing products without endangering human health) and Article 9 (2) (h) (processing is necessary for the purposes of preventive medicine).</p> <p>The respective medical, hygienic and production requirements are laid down, among others, in the European Pet Food Industry Federation's regulations (<a href="http://www.fediaf.org/self-regulation/nutrition/">http://www.fediaf.org/self-regulation/nutrition/</a>), and in the</p>	<p>The visitor's register shall include the purpose of the visit in the case of individuals visiting the relevant premises (work/meeting/customer's visit/official inspection/audit), in the case of work its description, date of visit, time of entry and exit, name and position of the individual, the company on whose behalf the visitor acts, type and serial number of camera and laptop if carried in (for reasons associated with the security of property and protection of confidential information, due to the protection of the same types of apparatuses of the Company and the information stored in them. By means of these actions, the Company may, for example, be able to prevent an apparatus of worse quality being carried in as a decoy, and a more valuable apparatus being carried out and misappropriated, that constitutes the property of the Company which may contain information that may be classified as confidential corporate</p>	<p><b>Data retention period: 3 years</b> (which period has been specified subject to the expiry data of the Company's products and for reasons associated with product safety.</p> <p><b>Authorised persons having access to the data within the Company:</b> employees of the security service department, quality manager, production manager, factory manager.</p> <p><b>Humannestor Kft.</b> (registered seat: 7187 Bonyhád-Majos, V. u. 71.), which is in charge of the security surveillance of the Company's premises, also has access to the data.</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
	Hungarian and EU legislation.	<p>information.)</p> <p>On one registration sheet only the employees/representatives of one single organisation (company) can be recorded.</p> <p>The aim of the entry statement is for the Company to ensure that, before entry to the plant, visitors do not cause contamination or do not pose a risk to the safety of its products. Accordingly, in line with the processing purposes above, the entry statement contains questions for the individual regarding the existence of illnesses or health hazards which may threaten the fulfilment of these purposes, as well as questions regarding any recent trips [to “developing nations, or countries/territories with a climate that significantly differs from that of the home country/ posing major risk of epidemic].</p>	
<b>Baggage screening for property protection purposes</b>	<p>Sections 25 (2), 26 (1) b)-c) and 28 (1) of Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators.</p> <p>Accordingly, when guarding any non-public facility of the client, security guards are entitled to request any person entering or exiting the premises to present his / her package or delivery</p>	The name, signature and further data recorded in the register of visitors of the person subject to inspection, type of inspection, findings, measures taken based on the findings of the inspection, statement(s) that may have been made by the relevant person in connection with the inspection and the measures taken; names and	Until the final and conclusive termination of legal proceedings initiated on the basis of the inspection (e.g. civil procedure, criminal proceeding). In the absence of such proceedings, <b>5 years</b> after the baggage screening (Section 6:22 (1) of the Civil Code – claims lapse in 5 years unless otherwise provided for in the Civil Code), or if an offence was committed, until its limitation period. Then the processed data will be deleted. The purpose of data retention is to have the documentation about

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
	<p>documents. Security guards are also entitled to request any person being on or exiting the premises to present the contents of his / her package, vehicle or freight consignment as provided for below. The security guard may demand to see the contents of a package, a vehicle, or a consignment with a view to discharging his / her contractual obligations regarding security, upon stating the reason and objective of the proposed action, if a) there are reasonable grounds to believe that the person carries on his / her person any article obtained by a criminal act or misdemeanour if that article falls within the security guard's scope of contractual liability for safeguarding; b) the person fails to surrender this article when so instructed; and c) it is necessary for the prevention or stopping of the illegal conduct. In the case of exercising the above rights of inspection, out of the means available for achieving the relevant purpose the method causing the least injury to personal freedom and personal rights shall be chosen.</p> <p>Article 6 (1) (f) of the GDPR (processing of the data is needed for pursuing the legitimate interests of the Company). The legitimate interest: protection of the Company's property (property protection).</p>	<p>record numbers and signatures of the contributing witnesses, name, job title and signature of the person in charge of the inspection and the name of the organisational unit where he/she is employed, and the date and place of the minutes taken (including the closure of the minutes).</p>	<p>the inspection available during the data retention period, to ensure the necessary information for official or legal proceedings initiated as a result of the inspection, etc.</p> <p>In the case of minutes closed with negative results, the data retention period is 1 year after the minutes are taken. The purpose of the storage is to have the documentation about the inspection with negative result available during the 1 year data retention period, to ensure the necessary information for official or legal proceedings initiated as a result of the negative inspection, etc.</p> <p>The retention period of data of the contributing witnesses and the person in charge of the inspection corresponds to the above.</p> <p><b>Authorised persons having access to the data within the Company:</b> employees of the security service department.</p> <p><b>Humannestor Kft.</b> (registered seat: 7187 Bonyhád-Majos, V. u. 71.), which is in charge of the security surveillance of the Company's premises also has access to the data.</p>
<b>Microsoft Teams and</b>	Article 6 (1) (f) GDPR (data processing	Content and information shared	Personal data will be stored until the end of the

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
<p><b>Stream services - using screen sharing, online communication, meeting, web and video conferencing, and video streaming services.</b></p>	<p>is necessary for the legitimate interests of the Company).</p> <p>The legitimate interest: to provide those partner communication channels, which are necessary for the normal conduct of business.</p>	<p>while using the services.</p>	<p>licensing of Microsoft Teams by the Company.</p> <p>Personal data will be stored until the end of the licensing of Microsoft Stream by the Company.</p>
<p><b>Verifying the proper use of the Company's email accounts.</b></p> <p><b>Employees of the Company may use their e-mail account in accordance with specific internal regulations. During the verification of proper use, the Company may have access to e-mails sent to the Company or its employees by external persons to the PPF e-mail address.</b></p>	<p>The legal basis for data processing is Article 6 (1) (f) of the GDPR (data processing is necessary to enforce the legitimate interests of the Company).</p> <p>Legitimate interest: to verify the proper use of the Company's e-mail account provided by the Company to the Company's employees, to protect the Company's trade secrets and intellectual property, to clarify liability for possible infringements, to prevent, assess damage, etc. related to a personal data breach or data loss.</p>	<p>The data traffic pertaining to the e-mail address, the senders of the incoming e-mails, the recipients of the e-mails sent, the e-mail headers, the content of the e-mails and any attachments.</p>	<p>The Company erases the data processed for verifying the regular use of the corporate email account <b>3 years</b> after the termination of the relevant employee's employment (general limitation period in HR matters).</p> <p>If, after the actual monitoring, the data is required, e.g. for the Company to pursue claims or defend itself against claims lodged by employees or third parties, or in any related court proceedings, or proceedings brought by an employee or third party before any authority, then data may, as the case may be, be retained beyond the above period until the final and binding conclusion of the above proceedings (for example until a final and binding judgement is delivered).</p> <p>In particular the key importance of the existence and monitoring of electronic correspondence in relation to business consultations, business development, products and the performance of obligations that the Company has vis-à-vis its business partners and the rights and claims of the Company serve to support the above.</p> <p><b>Persons within the Company who can access the data:</b> the General Manager, the members of the IT Department where the HR Department instructed them to do so, and the members of the</p>

Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
			HR Department proceeding in the given matter. Where there is an issue at stake which falls within the competence of the Company's superiors, they also may learn of and access the relevant data. In addition, the members of the Legal Department, who proceed in the given matter, may learn of and access the data related to the use of the e-mail accounts in connection with pursuing a possible claim, or the termination of the employment.
<p><b>Data processing related to the enforcement of the rights of individuals (see Clause 7 in detail)</b></p>	<p>Article 6 (1) (c) of the GDPR (processing is necessary for compliance with a legal obligation to which the Company as a controller is subject)</p> <p><b>Legal obligation:</b> to enable data subjects to exercise their rights set out in Articles 15-22 of the GDPR and document any other step taken in relation to inquiries.</p>	<p>Personal data related to inquiries received by the Company in respect of data protection: in the case of individuals / legal entities or other organisations contacting the Company, the data of the contact person necessary for making contact (including without limitation name, address, e-mail, phone), the content of the inquiry and steps taken and documents made in relation to the inquiry. For example, if an individual requests the deletion of all his/her data by email under the GDPR and the Company performs this request, then the email itself in which the individual requested deletion will nevertheless be kept.</p>	<p><b>Data retention period:</b> indefinite unless the data protection authority gives any other guidance.</p> <p><b>Persons authorised to access within the Company:</b> staff participating in responding to inquiries or requests and the representative of the Company.</p>
<p><b>Archiving the consents of individuals to data processing and the withdrawals of consents (if any)</b></p>	<p>Article 6 (1) (c) of the GDPR (processing is necessary for compliance with a legal obligation to which the Company as a controller is subject)</p> <p><b>Legal obligation:</b> Under Article 7 (1) of the GDPR where processing is based on</p>	<p>If any data processing of the Company is based on the consent of the data subject, the Company will archive the given consent. The purpose is to justify the lawfulness of the consent at any time. If the data subject withdraws</p>	<p><b>Data retention period:</b> indefinite unless the data protection authority gives any other guidance</p> <p><b>Persons authorised to access within the Company:</b> staff participating in handling consents and withdrawals of consents and the representative of the Company.</p>



Purpose of the processing	Legal basis of the processing	Scope of processed data	Data retention period, access rights, data transfers
	<p>consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.</p>	<p>his/her consent, the Company will retain the declaration of withdrawal (and the related communication). The purpose is to ensure that the Company is always aware of the fact that an individual has withdrawn his/her consent to a specific data processing.</p>	
<p><b>Keeping records of personal data breaches (including documenting steps taken in relation to responding to incidents)</b></p>	<p>Article 6 (1) (c) of the GDPR (processing is necessary for compliance with a legal obligation to which the Company as a controller is subject).</p> <p><b>Legal obligation:</b> Under Article 33 (5) of the GDPR the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the GDPR.</p>	<p>Personal data of the data subjects affected by the personal data breach.</p>	<p><b>Data retention period:</b> indefinite, unless the data protection authority gives any other guidance.</p> <p><b>Persons authorised to access within the Company:</b> staff participating in responding to personal data breaches and the representative of the Company.</p>

5. **DATA PROCESSORS**

The Company engages the following contractual partners for carrying out tasks related to data processing operations in addition to the ones listed above. Such contracting parties act as so-called “data processors” (i.e. they process the personal data defined in this Notice on behalf of the Company).

The Company should only use data processors that provide sufficient safeguards, in particular in terms of expertise, reliability and resources, for the implementation of technical and organisational measures which ensure that the requirements of the GDPR are met. Said safeguards should include the security of processing. The particular tasks and liabilities of the data processor are provided for in the data processing agreement made between the Company and the data processor. After the completion of the processing on behalf of the Company, the processor shall, at the choice of the Company, return or delete the personal data, unless there is a requirement to store the personal data under European Union or Member State law to which the processor is subject.

Data processor	Tasks
<b>Contracting partners participating in promotions and advertising campaigns (including prize games organised by the Company)</b>	The details of the data processor and its tasks are indicated in the terms and conditions of participation in the given promotion.
<b>External IT service providers of the Company</b>	Hosting services, system administration tasks, on-site support to end-users, maintenance of computers, managing user accounts and setting authorisations, operation of servers, checking backups, domain administration, provision of remote support in relation to the TSM system.
<p>IT service providers within the corporate group:</p> <p><b>Partner in Pet Food Polska SP.z.o.o.</b> ul. Szamocka 8, Warsaw 01-748, Poland telephone No: +48 22 569 24 10, <a href="mailto:info.pl@ppfeurope.com">info.pl@ppfeurope.com</a>,</p> <p><b>Partner in Pet Food CZ s.r.o.</b> Bucharova 1423/6 158 00 Prague 13 – Nové Butovice, Czech Republic telephone No: +420 234 111 111; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p><b>Partner in Pet Food SK s.r.o.</b> Kračanská cesta 40, 929 01 Dunajská Streda, Slovakia telephone No: +421 31 559 13 65; <a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p><b>Partner in Pet Food NL B.V.</b> Wijchenseweg 132 6538 SX Nijmegen, Holland telephone No: +31 24 34 35 910;</p>	<p>Provision of IT services on the basis of an indefinite-term service agreement.</p> <p>E.g.: central arrangement of the operation of the IT systems, preparation of back-up saves, protection of the company-wide network and preparations for data loss incidents. IT support of processes related to leaving and joining employees, managing user accounts, setting authorisations, blocking access to user accounts, archiving email accounts, remote deletion of mobile phones.</p>

Data processor	Tasks
<p><a href="mailto:info@ppfeurope.com">info@ppfeurope.com</a></p> <p><b>Doggy AB</b> (447 84 Vårgårda, Doggyvägen 1, Sweden)</p> <p><b>Bozita GmbH</b> (Osterfeldstraße 12-14, 22529 Hamburg, Germany)</p> <p><b>Landini Giuntini S.p.A.</b> (via Rosa Luxemburg n.30, 06012 Città di Castello (PG), Italy)</p> <p><b>Mispol S.A.</b> (ul. Octowa 1, 15 - 399 Białystok)</p> <p><b>Kalisz Pet Food Sp.z.o.o.</b> (ul. GRZYBOWSKA 2, lok. 29, Warsaw 00-131, Poland)</p>	
<p><b>Microsoft Teams and Stream services - screen sharing, online communication, meeting, web and video conferencing, and video streaming services.</b></p> <p><b>Microsoft Ireland Operations Ltd.</b> One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland</p> <p><b>Microsoft Corporation</b> One Microsoft Way Redmond, Washington 98052 USA</p> <p>Online contact: <a href="#">Ask questions about Microsoft privacy – Microsoft privacy</a></p>	<p>The Company may also use the personal data specified in this Notice in the course of its daily communications through Microsoft Stream video streaming provided by Microsoft, as well as Microsoft Teams screen sharing, online communication, meeting, web and video conferencing services.</p> <p>During the services, personal data may also be processed in non-EU countries that do not provide the appropriate level of data protection set by the GDPR. With respect to the collection, transfer and processing of personal data in non-EU member states, Microsoft Corporation provides for the personal data protection through standard contractual clauses approved by the EU Commission in decision 2021/914/EC, dated 4 June 2021.</p> <p>Further information:</p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview">https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview</a></p> <p><a href="https://www.microsoft.com/hu-hu/microsoft-365/microsoft-teams/security">https://www.microsoft.com/hu-hu/microsoft-365/microsoft-teams/security</a></p> <p><a href="https://docs.microsoft.com/hu-hu/stream/portal-permissions">https://docs.microsoft.com/hu-hu/stream/portal-permissions</a></p>
<p><b>Admagic Kommunikációs Kft.</b> 1015 Budapest, Széna tér 1/A telephone: +36 1 2247740 <a href="mailto:info@admagic.hu">info@admagic.hu</a></p>	<p>Responsible for implementing prize games. In the course of implementation, it has access to personal data processed by the Company in relation to prize games. Scope of data: surname, first name, e-mail address, postal code, town name, address, telephone number.</p> <p>Example of tasks: webpage programming, verification of receipts, drawing lots, collecting, inspecting, storing and handover to the Company of registrations during prize competition bound to purchase, prior to the competition</p>

Data processor	Tasks
	sending out eDM for information purposes. The data is deleted after the prize competition closes.
<p><b>Radex Media Group</b>  1113 Budapest, Vincellér utca 39/A  telephone: +36 1 788 0278  <a href="mailto:milan@radex.hu">milan@radex.hu</a></p>	<p><b>1. Database management related to sending newsletters, and sending out the actual newsletters</b></p> <p>In relation to the management of the database related to sending out newsletters: the data processor processes the personal data of individuals (name, e-mail) until the individual withdraws consent. (Subscribers have the possibility to unsubscribe from the newsletter, in this case the newsletter sending system automatically deletes their data. If a subscriber requests from the data processor by e-mail to be unsubscribed from the newsletter, then the data processor's staff shall delete his/her data from the database.) The data processor uses the newsletter dispatch function of Mad Mini to store the data of subscribers and send out newsletters. In respect of the security of data entered into here, the data processing principles of Mad Mini shall prevail.  <a href="https://uk.godaddy.com/agreements/privacy">https://uk.godaddy.com/agreements/privacy</a>.</p> <p><b>2. Database management related to conducting Facebook prize drawings</b></p> <p>On behalf of the Company the data processor organises and conducts weekly message board prize drawings on the PreVital Facebook page, in which winners are selected from among participants by machine. The names, addresses and telephone numbers that winners give voluntarily are then recorded. Based on this data, the prize packets are delivered to the winners by courier service. The goal is to send the prize packets to winners, so after the prize packets have been sent, as soon as the courier services forward the confirmation of the completion of deliveries, the processor provides the Company with the list of the winners and deletes the above data from its own systems.</p> <p>In addition: Comprehensive management of the PreVital Facebook page of the Company, including compiling the content, specifying advertisements and posts. The data processor can see fans' Facebook profiles and the content they have uploaded to the page. When a fan contacts the site via Messenger message, the winner's name, address, and phone number will be collected by the data processor from the conversation as described above. If a person reports a product complaint on Facebook, the data processor shall forward that complaint to the Company.</p>
<p><b>Humannestor Kft.</b>  <b>7187 Bonyhád-Majos, V.u. 71.</b></p>	<p>Providing security services under a service contract of indefinite duration - 2943 Bábolna, facility on plot with top. lot no. 108/2; 7361 Kaposszekcső, Dombóvár Industrial Park; 7200 Dombóvár, Borsos Miklós u. 1; Sopronhorpács unit (9463 Sopronhorpács, Fő utca 68.). Main tasks: inspecting personnel traffic, baggage screening, inspection at entry and</p>

Data processor	Tasks
	<p>exit.</p> <p>The service provider keeps a register of persons entering the Company's premises.</p>
<p><b>SFDC Ireland Limited</b>  The Atrium, Level 1, Block A  Sandyford Business Park Dublin 18  Ireland  <a href="https://www.salesforce.com/eu/?ir=1">https://www.salesforce.com/eu/?ir=1</a></p>	<p>Szerződéses partnerek vagy lehetséges szerződéses partnerek kapcsolattartóinak, és/vagy az ajánlatkérési / ajánlatadási folyamatba, szerződés teljesítésébe / szerződés teljesítésének ellenőrzésébe bevont személyek adatainak tárolása a Salesforce Sales Cloud rendszerében.</p>

## 6. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

The Company protects the personal data it processes primarily by restricting the access to the information and by clearly specifying users' rights. Only the persons who require access in order to fulfil the above-mentioned purposes and/or are authorised to have access are entitled to access the systems and instruments used for processing the personal data referred to in this Notice. These persons include, e.g., designated team members or departments (e.g. in respect of user data that are required for the use of the Company's IT systems, the IT Department).

The Company ensures the safe and legitimate use of the devices which it makes available (including Company-owned computers, notebooks and mobile phones), the e-mail accounts and the Internet, and the desired level of awareness of the employees related to such use by applying the following measures:

- The Company expects that the devices that it made available and that have access to the Internet as well as the e-mail accounts are used by the employees with specific user names and passwords which are adequately complex and up-dated at regular intervals.
- The Company protects all its systems and devices by fire wall, antivirus software and spam filters. In addition, the Company operates an intrusion protection system (so-called IPS) which enables the detection, blocking and logging of illegitimate attempts of intrusion into the computer systems of the Company.
- The Company makes safe wired and wireless network access available for all company devices provided by the Company.
- Remote access to the systems and software of the Company from any device is possible only through safe connection (VPN) by using specific user names and passwords, with mitigation of chances of accidental access (including illegitimate access by the use of stolen or lost devices).
- The IT Department of the Company carries out regular software and system up-dates and back-up saves of data in accordance with its own internal regulations.

As regards the physical protection of data and electronic documents, the Company owns locked server rooms and ensures that access to a particular document is reserved to adequately authorised persons only (e.g. access to HR documents is reserved to the HR Department, access to payroll data is reserved to the Financial Department and the data processor engaged for payroll accounting).

## 7. DATA PROTECTION RIGHTS AND REMEDIES

## **7.1 Data protection rights and remedies**

The detailed rights and remedies of the individuals are set forth in the applicable provisions of the GDPR (especially in Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80, and 82 of the GDPR). The summary set out below describes the most important provisions and the Company provides information for the individuals in accordance with the above articles about their rights and remedies related to the processing of personal data.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the individual, information may also be provided orally, provided that the identity of the individual is verified by other means.

The Company will respond without unreasonable delay to the request of an individual in which such person exercises his/her rights about the measures taken upon such request (see Articles 15-22 of the GDPR), with said response by no means to occur later than one month after receipt thereof. This period may, if needed, be extended for a further two months in light of the complexity of the request and the number of requests to be processed. The Company shall notify the individual about the extension and also indicate its grounds therefor within one month of the receipt of the request. Where the request has been submitted by electronic means, the response should likewise be sent electronically, unless the individual requests otherwise.

If the Company does not take any measure upon the individual's request, it shall so notify the individual without delay, but by no means later than one month after receipt thereof, stating why no measures will be taken. Additionally, the Company shall inform the individual about the individual's right to lodge a complaint with the data protection authority and to file an action for remedy with the courts.

## **7.2 The individual's right of access**

- (1) The individual has the right to obtain confirmation from the Company with regards to whether or not personal data concerning them is being processed. In such a case, the individual is entitled to have access to the relevant personal data and to the following information:
  - a) the purposes of the processing;
  - b) the categories of personal data concerned;
  - c) the recipients or categories of recipient to whom the personal data has been or will be disclosed, specifically including recipients in third countries and/or international organisations;
  - d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - e) the right of the individual to request from the Company rectification or erasure of personal data, or restriction of processing of personal data concerning the individual, or to object to such processing;
  - f) the right to lodge a complaint with a supervisory authority;
  - g) where the personal data is not collected from the individual, any available information as to its source.
- (2) Where personal data is forwarded to a third country, the individual is entitled to obtain information concerning the adequate safeguards of the data transfer.
- (3) The Company provides a copy of the personal data undergoing processing to the individual. The Company may charge a reasonable fee based on administrative costs for requested further copies thereof. Where the individual submitted their request by electronic means, the information will be provided to them in a commonly used electronic form unless otherwise requested by the data subject.

## **7.3 Right to rectification**

The individual has the right to request that the Company rectify inaccurate personal data which concerns them without undue delay. In addition, the individual is also entitled to have incomplete personal data completed e.g. by a supplementary statement or otherwise.

#### **7.4 Right to erasure ('right to be forgotten')**

- (1) The individual has the right to request that the Company erase the personal data concerning them without delay where one of the following grounds applies:
  - (a) the personal data is no longer required for the purposes for which it was collected or otherwise processed by the Company;
  - (b) the individual withdraws consent on which the processing is based, and there are no other legal grounds for the processing;
  - (c) the individual objects to the processing and there are no overriding legitimate grounds for the processing;
  - (d) the personal data has been unlawfully processed;
  - (e) the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject;
  - (f) the collection of the personal data occurred in connection with the offering of services regarding the information society.
- (2) If the Company has made the personal data public and it is later obliged to delete it as a result of the above stated grounds, it will take reasonable steps to delete it, taking into account the available technology and the costs of implementation. These reasonable steps include technical steps in order to inform processors who carry out processing that the individual has initiated a request for the links leading to the relevant personal data, or the copies or reproductions thereof, be deleted.
- (3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary, among other things, for:
  - a) exercising the right of freedom of expression and information;
  - b) compliance with a legal obligation which requires processing by European Union or Member State law to which the Company is subject;
  - c) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes insofar as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - d) the establishment, exercise, or defence of legal claims.

#### **7.5 Right to restriction of processing**

- (1) The individual has the right to obtain a restriction of processing from the Company where one of the following applies:
  - a) the accuracy of the data is contested by the individual, for a period enabling the Company to verify the accuracy of the personal data;
  - b) the processing is unlawful, and the individual opposes the erasure of the personal data and requests the restriction of its use instead;
  - c) the Company no longer needs the personal data for the purposes of the processing, but the individual requires it for the establishment, exercise or defence of legal claims;
  - d) the individual has objected to processing pending the verification of whether the legitimate grounds of the Company override those of the individual.
- (2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with consent of the individual or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

- (3) The Company informs the individual whose request has served as grounds for the restriction based on the aforesaid, before the restriction of processing is lifted.

#### **7.6 Notification obligation regarding rectification or erasure of personal data or restriction of processing**

The Company will communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if they so request.

#### **7.7 Right to data portability**

- (1) The individual has the right to receive the personal data concerning them, which they have provided to the Company in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller without hindrance from the Company, where:
  - a) the processing is based on consent or on a contract; and
  - b) the processing is carried out by automated means.
- (2) In exercising the right to data portability pursuant to paragraph (1), the individual shall have the right to have the personal data transmitted directly from one controller to another (thus from the Company to another controller), where technically feasible.
- (3) Exercising the aforesaid right shall be without prejudice to provisions concerning the right to erasure ('right to be forgotten') and, further, this right shall not adversely affect the rights and freedoms of others.

#### **7.8 Right to object**

- (1) **The individual has the right to object, on grounds relating to his/her particular situation, at any time to the processing of personal data concerning them for the purposes of legitimate interests. In such a case, the Company will no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the individual, or for the establishment, exercise or defence of legal claims.**
- (2) **Where the processing of personal data serves direct marketing purposes the individual is entitled to object to the processing of personal data regarding them for such purposes, including profiling, in so far as the latter relates to direct marketing.**
- (3) If the individual objects to the processing of personal data with the aim of direct marketing, then the personal data can no longer be processed for this purpose.
- (4) In connection with the use of services related to information society, the individual may resort to their right of objection, with deviation from Directive No 2002/58/EC, by means of automated devices based on technical requirements.
- (5) Where personal data is processed for scientific or historical research purposes or statistical purposes, the individual, on grounds relating to their particular situation, has the right to object to the processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

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



The individual has the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement if they consider that the processing of personal data relating to them infringes the GDPR. In Hungary, the competent supervisory authority is the Hungarian Authority for Data Protection and Freedom of Information (<http://naih.hu/>; address: 1055 Budapest, Falk Miksa utca 9-11.; postal address:1363 Budapest, Pf.: 9; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu))

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

- (1) The individual has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
- (2) The individual has the right to an effective judicial remedy where the supervisory authority that is competent does not handle a complaint or does not inform them within three months on the progress or outcome of the complaint lodged.
- (3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

#### **7.11 Right to an effective judicial remedy against the Company or the processor**

- (1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, any individual has the right to an effective judicial remedy where they consider that their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR.
- (2) Proceedings against the Company or a processor shall be brought before the courts of the Member State where the Company or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence. In Hungary, the general court has jurisdiction in these kinds of proceedings. The proceedings can be brought - according to the choice of the individual concerned - before the general court where one has its habitual residence or place of stay. Information on the competent courts and their contact details is available at [www.birosag.hu](http://www.birosag.hu).