Table of contents

Peiko Dogwear Ltd.

Peiko.com Privacy Policy

Introduction

Peiko Dogwear Kft. (1124 Budapest, Deres utca 13 3. 7., tax number: 27785353-2-43, company registration number/register number: 01-09-397791) (hereinafter referred to as the "Service Provider", "Data Controller") hereby declares that it is subject to the following policy:

Pursuant to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation) (27 April 2016), the following information is provided.

This Privacy Policy governs the processing of data on the following website: https://Peiko.com/

The Privacy Policy is available at: https://Peiko.com/adatvedelem, https://Peiko.com/privacy-policy

Amendments to this policy will enter into force upon publication at the above address.

The contact details of the data controller

Name: Peiko Dogwear Ltd.

Address: 13 Deres Street 3/7, Budapest, H-1124, Hungary

E-mail: info@peiko.com

Phone: +36 30 538 53 18

Definitions of terms

(1)"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'controller' means a natural or legal person, public authority, agency or any other body which is responsible for the processing of personal data

where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for the designation of the controller may also be determined by Union or Member State law;

(4) 'processor' means a natural or legal person, public authority, agency or any other body,

a public authority, a public sector body or an agency or any other body which processes personal data on behalf of the controller;

(5) 'recipient' means a natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. Public authorities that may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

(6) 'consent of the data subject' means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data relating to him or her;

(7) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

Principles on the processing of personal data

Personal data:

1. be processed lawfully and fairly and in a transparent manner for the data subject ("lawfulness, fairness and transparency");

2. be collected only for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original purposes in accordance with Article 89(1) ('purpose limitation');

3. the processing must be adequate, relevant and necessary for the purposes for which it is carried out

necessary ("data minimisation");

4. accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without undue delay ('accuracy');

5. be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods only if the personal data will be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1),

subject to the implementation of appropriate technical and organisational measures as provided for in this Regulation to safeguard the rights and freedoms of data subjects ('limited storage');

6. be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ('integrity and confidentiality'), by implementing appropriate technical or organisational measures.

The controller is responsible for compliance with the above and must be able to demonstrate such compliance ("accountability").

The controller declares that its processing is in accordance with the principles set out in this point.

Data processing related to the operation of the webshop/use of the service

1. Fact of data collection, scope of data processed and purpose of data processing:

Personal data	Purpose of processing	Jogalap
Username	Identification, Enabling registration.	Article 6(1)(b) of the GDPR and Section 13/A(3) of the Elker Act.
Password	Used for secure access to the user account.	
First and last name	It is necessary for contacting you, making a purchase, issuing a proper invoice, exercising the right of withdrawal.	
E-mail address	Contact	
Phone number	Liaising, negotiating invoicing or delivery issues more efficiently.	
Billing name and address:	The issuing of proper invoices, the creation, definition, modification, monitoring of the performance of the contract, the invoicing of the resulting fees and the related enforcing claims in connection therewith.	Article 6(1)(c) and on accounting Act C of 2000 on accounting § 169 (2)
Shipping name and adress	The possibility of home delivery	Article 6 (1) of the GDPR paragraph (b) and the Elker tv. § 13/A (3) para.
Date of registration/purchase	perform a technical	

	operation		

2. Stakeholders: all data subjects registered/customers of the webshop website.
3. Neither the username nor the e-mail address need to contain personal data.
4. Duration of processing, time limit for erasure of data: If one of the conditions of Article 17(1) of the GDPR applies, it will last until the data subject's request for erasure. The controller shall inform the data subject of the erasure of any personal data provided by the data subject by electronic means pursuant to Article 19 of the GDPR. If the data subject's request for erasure also includes the e-mail address provided by him or her, the controller shall erase the e-mail address following the notification. Except in the case of accounting records, since pursuant to Article 169 (2) of Act C of 2000 on Accounting, these data must be kept for 8 years. The contractual data of the data subject may be deleted after the expiry of the civil law limitation period on the basis of a request for deletion by the data subject.
   The accounting documents (including general ledger accounts, analytical or detailed records) directly and indirectly supporting the accounting accounts must be kept for at least 8 years in a legible form, retrievable by reference to the accounting records.

5. Identity of the potential data controllers, recipients of personal data : Personal data may be processed by the data controller and its sales and marketing staff, in compliance with the above principles.
6. Description of data subjects' rights in relation to data processing:
   a. The data subject may request the controller to access, rectify, erase or restrict the processing of personal data relating to him or her, and
   b. the data subject has the right to data portability and the right to withdraw consent at any time to withdraw it at any time.
7. Data subjects may request access to, erasure, modification, restriction of processing, portability or objection to the processing of their personal data in the following ways:
   a. By post to 1124, Budapest, Deres utca 13, 3.7,
   b. Via e-mail to: info@peiko.com
   c. Via phone: +3630 538 53 18
8. Legal basis for data processing:
   a. Article 6(1)(b) and (c) of the GDPR,
   b. Section 13/A(3) of Act CVIII of 2001 on electronic commerce and electronic commerce-related matters (hereinafter referred to as the "Elker Act"):
      The service provider may process personal data which are technically indispensable for the provision of the service. The service provider must, other things being equal, choose and in any case operate the means used in the provision of the information society service in such a way that personal data are processed only if absolutely necessary for the provision of the service and for the fulfilment of the other purposes specified in this Act, but in this case only to the extent and for the duration necessary.
   c. in the case of invoicing in accordance with accounting legislation, Article 6(1)(c).

d. in the case of enforcement of claims arising from the contract, 5 years pursuant to § 6:22 of Act V of 2013 on the Civil Code.

§ 6:22 [Limitation period]
(1) Unless otherwise provided by this Act, claims shall be time-barred after five years.
(2) The limitation period shall begin to run when the claim becomes due.
(3) An agreement to change the limitation period shall be in writing.
(4) An agreement excluding the limitation period is void.

9. Please be informed that

a) The processing is necessary for the performance of the contract and the offer.
b) Failure to provide the data will result in our inability to process your order.

Cookie policy

1. The so-called "password-protected session cookie", "shopping cart cookies", "Security cookies", "Necessary cookies", "Functional cookies", and "cookies used to manage website statistics cookies for website statistics" do not require the prior consent of the data subject.
2. Fact of processing, scope of data processed: unique identifier, dates, times
3. Data subjects: all data subjects visiting the website.
4. Purpose of data processing: to identify users and track visitors
5. Duration of data processing, deadline for deletion of data:

Type of Cookie	Legal basis for processing	Duration of data processing
Session cookies	Paragraph 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elkertv.)	Until the close of the session
Funkcitional cookies	Paragraph 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elkertv.)	Until the deletion by data subject
Statistics and marketing cookies	Paragraph 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elkertv.)	1 month- 2 years

6. Who are the potential controllers of the data: no personal data are processed by the controller through the use of cookies.
7. Description of data subjects' rights in relation to data processing: data subjects have the possibility to delete cookies in the Tools/Preferences menu of their browsers, usually under the Privacy settings.
8. Legal basis for processing: no consent is required from the data subject where the sole purpose of the use of cookies is the transmission of communications over an electronic

communications network or where the use of cookies is strictly necessary for the provision of an information society service expressly requested by the subscriber or user.

9. Most browsers used by our users allow you to set which cookies should be saved and allow (certain) cookies to be deleted again. If you restrict the saving of cookies on specific websites or do not allow third party cookies, this may in certain circumstances lead to our website no longer being fully usable. Here you will find information on how to customise your cookie settings for standard browsers:

   Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)

   Internet Explorer (https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies)

   Firefox (https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn)

   Safari (https://support.apple.com/hu-hu/guide/safari/sfri11471/mac)

Using Google Ads conversion tracking

1. The data controller uses the online advertising program "Google Ads" and makes use of Google's conversion tracking service within its framework. Google Conversion Tracking is an analytics service provided by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA ("Google").
2. When you reach a website through a Google ad, a cookie is placed on your computer to track conversions. These cookies have a limited validity and do not contain any personal data, so they do not identify the User.
3. When the User browses certain pages of the website and the cookie has not expired, Google and the data controller may see that the User has clicked on the advertisement.
4. Each Google Ads client receives a different cookie, so they cannot be tracked through Ads clients' websites.
5. The information obtained through the use of conversion tracking cookies is used to provide conversion statistics to Ads' customers who opt for conversion tracking. Customers are thus informed of the number of users who click on their ad and are referred to a page with a conversion tracking tag. However, they do not have access to information that would allow them to identify any user.
6. If you do not wish to participate in conversion tracking, you can opt-out by disabling the option to set cookies in your browser. You will then not be included in the conversion tracking statistics.
7. Further information and Google's privacy statement can be found on the following page: www.google.de/policies/privacy/

Using Google Analytics

1. This website uses Google Analytics, a web analytics service provided by Google Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site you have visited.
2. The information generated by the cookies on the website used by the User is usually transmitted to and stored on a Google server in the USA. By activating the IP anonymisation on the website, Google will previously shorten the User's IP address within the Member States of the European Union or in other states party to the Agreement on the European Economic Area.
3. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. Google will use this information on behalf of the operator of this website to evaluate your use of the website, to compile reports on website activity for the website operator and to provide other services relating to website activity and internet usage.
4. The IP address transmitted by the User's browser within the framework of Google Analytics will not be merged with other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. You may also prevent Google from collecting and processing information about your use of the website (including your IP address) by means of cookies by downloading and installing the browser plug-in available at https://tools.google.com/dlpage/gaoptout?hl=hu

Recipients to whom personal data are disclosed

"recipient" means a natural or legal person, public authority, agency or any other body to whom or with which personal data is disclosed, whether or not a third party.

1. Processors (who carry out processing on behalf of the controller)

The data controller uses data processors to facilitate its own data processing activities and to fulfil its contractual and legal obligations with data subjects.

The controller shall place great emphasis on using only processors that provide adequate guarantees to implement appropriate technical and organisational measures to ensure compliance with the requirements of the GDPR and to protect the rights of data subjects.

The processor and any person acting under the control of the controller or the processor who has access to the personal data shall process the personal data covered by this Policy only in accordance with the instructions of the controller.

The controller shall be legally responsible for the activities of the processor. A processor shall be liable for damage caused by processing only if it has failed to comply with the obligations specifically

imposed on processors by the GDPR or if it has disregarded or acted contrary to lawful instructions from the controller.

The processor has no substantive decision-making power with regard to the processing of the data.

The data controller shall use a hosting service provider to provide the IT background, a delivery service provider to deliver the products ordered as data processor.

Data processing activity	Name and contact
Hosting service	WP Online Magyarország Kft. 1094, Budapest, Balázs Béla utca 15-21 D204
Other services	Mailchimp (https://mailchimp.com/ ; The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA) ; Szamlazz.hu (KBOSS. hu Kft., 1031 Budapest, Záhony utca 7., info@szamlazz.hu) WP Online Magyarország Kft (https://wpo.hu/hu/ 1094 Budapest, Balázs Béla utca 15-21. D. lház. 2. em. 4.

"third party" means a natural or legal person, public authority, agency or any other body which is not the same as the data subject, the controller, the processor or the persons who are under the direct authority of the controller or processor.

Transfer of data to third parties

Third party data controllers process the personal data we provide on their own behalf and in accordance with their own privacy policies.

Data processing	name and contact details
Delivery service	*GLS General Logistics Systems Hungary Csomag-logisztikai Kft.* *2351 Alsónémedi, GLS európa u 2.*
Online payment	OTP Simple Pay https://simplepay.hu/ Telefonszám: +36 1 5100 374 OTP Mobil Kft. 1143 Budapest, Hungária krt. 17-19. ugyfelszolgalat@simple.hu ; PayPal enquiry@paypal.com PayPal (Európa) S.à r.l. et Cie, S.C.A. 22-24 Boulevard Royal L-2449

	Luxemburg Cégjegyzékszám: R.C.S. Luxembourg B 118 349

Customer relations and other data management

1. Should the data controller have any questions or problems when using our services, the data subject may contact the data controller using the methods provided on the website (telephone, e-mail, social networking sites, etc.).
2. The Data Controller shall delete the data provided in e-mails, messages, telephone, Facebook, etc., together with the name and e-mail address of the interested party and other personal data voluntarily provided by the interested party, after a maximum of 2 years from the date of the communication.
3. Information on data processing not listed in this notice is provided at the time of collection.
4. The Service Provider shall be obliged to provide information, disclose data, hand over data or make documents available in response to exceptional requests from public authorities or other bodies authorised by law.
5. In such cases, the Service Provider shall disclose personal data to the requesting party only to the extent and to the extent strictly necessary for the purpose of the request, provided that the requesting party has indicated the exact purpose and scope of the data.

Rights of data subjects

1. **Right of access**

You have the right to receive feedback from the controller as to whether or not your personal data are being processed and, if such processing is taking place, the right to access your personal data and the information listed in the Regulation.

2. **The right to rectification**

You have the right to have inaccurate personal data relating to you corrected by the controller without undue delay at your request. Taking into account the purposes of the processing, you have the right to request the rectification of incomplete personal data, including by means of a supplementary declaration.

3. **Right to erasure**

You have the right to obtain from the controller the erasure of personal data concerning you without undue delay and the controller is obliged to erase personal data concerning you without undue delay under certain conditions.

4. **The right to be forgotten**

If the controller has disclosed the personal data and is under an obligation to erase it, it will take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the controllers that process the data that you have requested the erasure of the links to or copies of the personal data in question.

5. **Right to restriction of processing**

You have the right to have the controller restrict processing at your request if one of the following conditions is met:

- You contest the accuracy of the personal data, in which case the restriction applies for the period of time that allows the controller to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the data and instead request the restriction of their use;
- the controller no longer needs the personal data for the purposes of the processing but you require them for the establishment, exercise or defence of legal claims;
- you have objected to the processing; in this case, the restriction shall apply for a period of time until it is established whether the controller's legitimate grounds override your legitimate grounds.

6. . The right to data portability

You have the right to receive the personal data concerning you that you have provided to a controller in a structured, commonly used, machine-readable format and the right to transmit these data to another controller without hindrance from the controller to whom you have provided the personal data (...)

7. The right to object

In the case of processing based on legitimate interest or public authority as legal grounds, you have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data by (...), including profiling based on the aforementioned provisions.

8. Objection in the case of direct solicitation

If personal data is processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such purposes, including profiling, where it is related to direct marketing. If you object to the processing of your personal data for direct marketing purposes, your personal data may no longer be processed for those purposes.

9. Automated decision-making in individual cases, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

The previous paragraph does not apply where the decision:

- necessary for the conclusion or performance of a contract between you and the controller;
- it is permitted by Union or Member State law applicable to the controller which also lays down appropriate measures to protect your rights and freedoms and legitimate interests; or
- is based on your explicit consent.

Deadline for action

The controller shall inform you of the action taken on such requests without undue delay and in any event within 1 month of receipt of the request.

If necessary, this can be extended by 2 months. The data controller will inform you of the extension, stating the reasons for the delay, within 1 month of receipt of the request.

If the controller fails to act on your request, it will inform you without delay and at the latest within one month of receipt of the request of the reasons for the failure to act, of the possibility to lodge a complaint with a supervisory authority and of your right to judicial remedy.

Security of data processing

The controller and the processor shall implement appropriate technical and organisational measures, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, in order to ensure a level of data security appropriate to the level of risk, including, where appropriate:

1. the pseudonymisation and encryption of personal data;
2. the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;
3. in the event of a physical or technical incident, the ability to access and use personal data data availability can be restored in due time;
4. the effectiveness of the technical and organisational measures taken to ensure the security of processing
   a procedure for the systematic testing, assessment and evaluation of.
5. The data processed must be stored in a way that does not allow unauthorised access. In the case of paper-based data carriers, by establishing physical storage and filing arrangements, and in the case of data in electronic format, by using a centralised access management system.
6. The method of storing the data by computerised means must be chosen in such a way that they can be erased, also taking into account any different erasure deadline, at the end of the erasure deadline or if otherwise necessary. Erasure shall be irreversible.
7. Paper-based data media should be shredded or personal data should be removed by an external organisation specialised in shredding. In the case of electronic data media, physical destruction and, where necessary, prior secure and irretrievable deletion of the data shall be ensured in accordance with the rules on the disposal of electronic data media.
8. The controller will take the following specific data security measures:

In order to ensure the security of personal data processed on paper, the Service Provider applies the following measures (*physical protection*):

1. Store the documents in a secure, lockable, dry place.
2. Where personal data processed on paper are digitised, the rules applicable to digitally stored documents apply
3. The Service Provider's data processing employee may leave the premises during the course of his/her work only if.
   processing is taking place, by locking up the data media entrusted to it or by closing the premises.

4. Personal data can only be accessed by authorised persons and not by third parties.
   have access to.
5. The Service Provider's building and premises are equipped with fire and property protection
   equipment.

IT security

1. Computers and mobile devices (other data carriers) used in the course of data processing
   are the property of the Service Provider.
   are.
2. The computer system containing personal data used by the Service Provider is protected
   against viruses.
3. To ensure the security of digitally stored data, the Service Provider uses data backups and
   archiving.
4. Access to the central server machine is only allowed to authorised and designated persons.
5. Access to data on computers is only possible with a username and password.

Informing the data subject about the personal data breach

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

The information provided to the data subject shall **clearly and prominently** state the nature of the personal data breach and provide the name and contact details of the data protection officer or other contact person who can provide further information; describe the likely consequences of the personal data breach; describe the measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The data subject need not be informed if any of the following conditions are met:

- the controller **has implemented appropriate technical and organisational protection measures** and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the **data unintelligible** to persons not authorised to access the personal data;
- the controller has taken additional measures following the personal data breach to **ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise**;
- information **would require a disproportionate effort**. In such cases, the data subjects should be informed by means of publicly disclosed information or by a similar measure which ensures that the data subjects are informed in an equally effective manner.

If the data controller has not yet notified the data subject of the personal data breach, the supervisory authority may, after having considered,
whether the data breach is likely to result in a high risk, may order the data subject to be informed.

Reporting a data breach to the authority

The data protection incident shall be notified by the controller to the supervisory authority competent under Article 55 without undue delay and, where possible, no later than 72 hours after the data protection incident has come to its attention, unless the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it shall be accompanied by the reasons justifying the delay.

Review in case of mandatory data processing

If the duration of the mandatory processing or the periodic review of its necessity is not specified by law, local government regulation or a binding legal act of the European Union, **the controller shall review, at least every three years from the start of processing, whether** the processing of personal data processed by the controller or by a processor acting on its behalf or under its instructions is **necessary** for the purposes of the processing.

The data controller shall **document the** circumstances and the results of this review**, keep this documentation for ten years after the review** and make it available to the National Authority for Data Protection and Freedom of Information (hereinafter referred to as "the Authority") upon request.

Complaint possibility

Complaints against possible infringements by the data controller can be lodged with the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information

1055 Budapest, Falk Miksa utca 9-11.

Address for correspondence: 1363 Budapest, Pf. 9.

Phone: +36 -1-391-1400

Fax: +36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

Closing words

The following legislation has been taken into account in the preparation of this information:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation) (GDPR) (27 April 2016);
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of

Information (hereinafter: Infotv.);

- Act CVIII of 2001 - on certain aspects of electronic commerce services and information society services (in particular § 13/A);
- Act XLVII of 2008 - on the prohibition of unfair commercial practices against consumers;
- Act XLVIII of 2008 - on the basic conditions and certain restrictions of economic advertising activities (in particular the
6.§a);
- Act XC of 2005 on Freedom of Electronic Information;