PRIVACY POLICY on the protection of personal data by Błonie Sp. z o.o.

Dear enthusiast of timeless watchmaking!

On May 25, 2018, the provisions of the PARLIAMENT REGULATION came into force OF THE EUROPEAN COUNCIL AND OF THE COUNCIL (EU) 2016/679 of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation, or GDPR).

By correspondence via the contact form and by subscribing to our newsletter posted on our website, as well as by sending us messages. You can provide us with your data by e-mail to e-mail addresses (...) @ zegarkiblonie.pl personal. In this situation, we become the Administrator of (your) Personal Data.

Błonie Sp. z o.o. (hereinafter Błonie) adjusted organizational and technical security measures for processing of personal data entrusted to us by you as part of our business.

We are committed to maintaining a high standard of data protection and full transparency processing of personal data entrusted to us, therefore we provide you with synthetic information about the processed personal data and related rights.

If you have any questions about the scope of GDPR (General Data Protection Regulation) implementation in Błonie, please contact us by e-mail at blonie@zegarkiblonie.pl or in writing, by traditional mail, to the following address: BŁONIE Sp.o.o., ul. ALEJA PRYMASA TYSIACLECIA 48A, 01-242 Warsaw.

Your Rights towards the Personal Data Administrator (hereinafter "Administrator" or "ADO" are following:

Right of access by the data subject: Article 15 of GDPR
1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and 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 have been or will be disclosed, in particular recipients in third countries 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 existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Right to rectification: Article 16 of GDPR

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten'): Article 17 of GDPR

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far 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

(e) for the establishment, exercise or defence of legal claims.

Right to restriction of processing: Article 18 of GDPR

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent 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. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Right to data portability: Article 20 of GDPR

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Right to object: Article 21 of GDPR

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

You can exercise these rights in any way, including by e-mail at address: blonie@zegarkiblonie.pl

The most important provisions of the Błonie Security Policy:

As part of its activities, Błonie performs the obligations arising from the GDPR depending on the scope data processing as the Personal Data Administrator or the Data Processor under the contract. In order to adapt internal procedures related to processing personal data for GDPR, a number of activities were carried out, including:

1) the Personal Data Protection Inspector (DPO) has been appointed,

2) the resource of personal data was reviewed in order to carry out new ones documents and specification of technical measures that meet the requirements of the GDPR and DPO,

3) the employees were trained in the scope of the new provisions of the GDPR and admission was ensured to process data only authorized persons and it has been ensured that persons authorized to process personal data undertook to keep unlimited secrecy, as well as keep records of persons authorized to processing of data entrusted to the processor,

4) impact assessments of the planned data processing operations were carried out before starting their processing (risk analysis - Article 35 of the GDPR),

5) a register of personal data protection processing activities has been established,

6) a system for reporting personal data breaches to the authority has been established supervisory and notifying about it to the data subjects (Articles 33 and 34 of the GDPR),

7) the Administrator was immediately informed that the data subject, sent to the Processor correspondence containing the request in the scope exercise the rights referred to in Chapter III of the GDPR, as well as share the content of this correspondence,
8) it has been ensured that the Administrator is provided with all the information necessary to prove its fulfillment of the obligations set out in art. 28 of the GDPR and made possible by the Administrator or an auditor authorized by the Administrator to conduct audits, incl inspecting and contributing to them,
9) all technical and organizational measures required under art. 32 GDPR, to ensure the level of security of data processing corresponding to the risk violation of the rights or freedoms of data subjects, in particular: pseudonymization or encryption of personal data, the ability to continuously ensure the confidentiality, integrity, and availability of systems and data processing services, the ability to quickly restore personal data and access them when a physical or technical incident, regularly testing, measuring and evaluating the effectiveness of technical measures in organizational to ensure the security of processing;

The data protection security policy contains a detailed description of the scope of duties and procedures in the proper management of information security in Błonie. Security should be understood as the actual state that prevents use that is inconsistent with the GDPR, flow, modification and / or destruction of personal data of which Błonie is the Administrator. The key arrangements in this regard include:

- securing the premises against access by third parties (security office, identification customers, access codes, IT security),
- appointing the DPO (responsible for supervision in terms of circulation and use documentation and data as well as technical and organizational conditions in which they are processed),
- systematic training of employees in the field of data processing and ways to protect them, periodic risk assessment of threats to data processing areas,
- control of compliance with the principles of data processing security and protection
- different levels of data access authorizations for each member of the Błonie team, each member of the Błonie team is obliged to sign an internal declaration confidentiality, in terms of all data obtained and processed in the course business activity conducted by Błonie.

The IT System Management Instruction for Data Processing constitutes a detailed specification of the Data Protection Security Policy conducted by Błonie. The intensive development of computer systems, applications and digitization of information causes that the data we collect is stored on storage devices (server), co allows all authorized members of the Błonie team to have access to them. To increase reliability and minimize the risk of data loss and / or access by unauthorized persons Błonie vw implemented appropriate IT security in this area. Risk of loss information (including obtained documents / databases, etc.) has been mitigated by:

- access passwords (to the operating systems of the company's employees' computers, to the server on which the data is stored, to the e-mail of company servers, files / documents containing sensitive data).
- Passwords consist of at least 8 characters, contain lowercase and uppercase letters and numbers and / or special characters, the same characters do not appear next to each other more than twice, users are required to change the password every 90 days, computers are equipped to turn on 15 minutes after the work is interrupted screensavers of monitors - the display is resumed only after entering the appropriate password,
- a binding ban on making copies of the entire Data Sets Entire Datasets can be copied only by the System Administrator or automatically by the System IT,
- in compliance with Data protection procedures,possibility of single copying of information onto magnetic,
- optical and other carriers only after encrypting the access to the data stored on them. Carriers are stored in locked cabinets. After the usefulness of these copies has expired,
- The data is permanently deleted or physically damaged media,
- the backup and data archiving system secures the manufactured products from the implementation research,
- RAID disk arrays and UPS, programs that control processes and access to files created during the run research,
- limiting the use of non-durable information carriers,
- firewall and antivirus protection (control of all incoming and outgoing data - including email, web traffic, and all interactions network).

The above tools result in the risk of losing the accumulated money at every stage of our business information material and / or unauthorized access to it will be limited as much as possible.
Useful information: General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj