PERSONAL DATA PROTECTION POLICY

1. This **"Personal data protection policy"** (hereinafter **"Policy"**) presents the requirements, rules and regulations regarding personal data protection adopted at the company operating under the business name BPH - British Publishing House Spółka z ograniczoną odpowiedzialnością with its registered seat in London SE10BL 72 Great Suffolk Street, holder of KRS No. 08659692 (hereinafter **"Company"**), in connection with the entry into force of the GDPR – Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union, L 119/1). The Company, the organisational unit responsible for information security, organisational units processing significant amounts of personal data, other organisational units as well as all staff members of the Company are responsible for compliance with this Policy. The Company will endeavour to ensure compliance of the Company's business partners with this Policy in an appropriate scope when personal data are transferred to them by the Company.

2. This policy includes:
   a. a description of data protection rules in force at the Company;
   b. procedures and instructions regarding individual areas in the field of personal data protection which require clarification made in separate documents.

3. The Policy was adopted by way of a resolution of the Management Board of the Company of 25 May 2018. The Management Board of the Company is responsible for the implementation of this Policy and its compliance within the Company.

4. **ABBREVIATIONS AND DEFINITIONS:**
   a. "**GPDR" –** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union, L 119/1).
   b. **"Data" –** mean personal data, unless the context suggests otherwise.
   c. "**Sensitive data**" – mean special data and criminal data.
   d. "**Special data**" – mean data listed in Article 9 (1) of the GDPR , i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
   e. "**Criminal data**" – mean data listed in Article 10 of the GDPR, i.e. data on convictions and offences.
   f. "**Data of children**" – mean data of persons under 16 years of age.
   g. **"(Data) Subject" –** means the data subject, unless the context suggests otherwise.
   h. **"Processor" –** means the organisation or person entrusted with the processing of personal data by the Company (e.g. the IT service provider, external accounting).
   i. **"Profiling" –** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
   j. **"Data export" –** means the transmission of data to a third country or an international organisation.
   k. **"DPO"** or **"Officer" –** means the Data Protection Officer

l. "**Record" –** means the Record of Data Processing Activities

5. PERSONAL DATA PROTECTION IN THE COMPANY – GENERAL RULES

5.1. Basic data protection rules in force at the Company:

a. **Legality** − The Company cares for privacy protection and processes data in accordance with the law.
b. **Security** − The company ensures an appropriate level of data security by constantly taking action in this area.
c. **Rights of Individuals** − The Company enables the people whose data is processed, to exercise their rights provided for in the GDPR and implement these rights.
d. **Accountability** − the Company documents the manner in which it fulfils its obligations regarding personal data protection in order to be able to demonstrate compliance with the GDPR at any time.

5.2. Principles of personal data processing by the Company

The Company processes personal data while respecting the following principles:

a. based on a legal basis and in accordance with the law (legalism);
b. honestly and fairly (reliability);
c. in a manner which is transparent for the data subject (transparency);
d. for specific purposes and not "just in case" (minimisation);
e. not more than necessary (adequacy);
f. with care for the correctness of data (correctness);
g. no longer than necessary (temporality);
h. ensuring proper data security (security).

5.3. Data protection system

The personal data protection system in the Company consists of the following elements:

1) **Stocktaking of data.** The Company identifies personal data resources in the Company, data classes, relationships between data resources, identification of data usage methods (stocktaking), including:
   a. cases of processing of special data and "criminal" data (**sensitive data**);
   b. cases of processing data of persons, whom the Company does not identify (**unidentified data**/UFO);
   c. cases of processing data of children;
   d. profiling;
   e. joint controlling of data.

2) **Record.** The Company develops, runs and maintains a Record of Data Processing Activities carried in the Company (hereinafter "Record"). The Record is a tool for accounting for compliance with data protection in the Company.
3) **Legal grounds.** The Company ensures, identifies and verifies the legal grounds for data processing, as well as:
   a. maintains a system for managing consents to data processing
   b. ensures stocktaking and providing details of the justification for cases when the Company processes data based on the Company's legitimate interest.

4) **Observing of rights of individuals.** The Company fulfils information obligations towards the data subject, and ensures that their rights are observed, thus implementing the requests received in this regard, including:
    a. **Information obligations.** The Company provides the persons with information required in the collection of data and in other situations where it is required by the GDPR and provides documentation of the implementation of these obligations.
    b. **The ability to perform requests.** The Company ensures the possibility of effective performance of any type of legitimate demand by itself and its processors.
    c. **Handling of requests.** The Company ensures appropriate expenditure and procedures to ensure that the requests of data subjects are handled on dates and in the manner required by the GDPR and properly documented.
    d. **Reporting breaches.** The Company uses procedures to determine the need to notify the subjects affected by the identified data protection breach.

5) **Minimalisation.** The Company applies the principles and methods of managing minimisation (privacy by default), including:
    a. principles of data **adequacy** management;
    b. principles of regulation and management of **access** to data;
    c. rules for managing the period of data storage and verification of further suitability.

6) **Security.** The Company ensures an appropriate level of data security, including:

    a. carries out risk analyses for data processing activities or their categories;
    b. conducts impact assessments for data protection where the risk of violation of rights and freedoms is high;
    c. adapts data protection measures to a specified risk;
    d. has an information security management system in place;
    e. uses procedures to identify, assess and report identified data breaches to the Data Protection Authority − it manages incidents.

7) **Processor.** The Company has rules in place regarding the selection of processors processing data for the Company, rules for determining requirements as to the terms of processing (entrustment agreements/processing rules, etc.), rules for verifying the performance of entrustment contracts (controls / audits, etc.).

8) **Data export.** The Company has rules in place for verifying whether the Company does not transfer data to third countries (i.e. outside the EU, Norway, Liechtenstein, Iceland) or to international organisations and to ensure the lawful terms of such transfers, if any.

9) ***Privacy by design*.** The Company manages changes in the scope of data processing affecting privacy. To this end, the procedures for launching new projects and investments in the Company take into account the need to assess the impact of changes on data protection, ensuring privacy (including compliance of processing goals, data security and minimisation) already at the design stage of the change, investment or at the beginning of a new project.
10) **Cross-border processing.** The Company has rules in place for verification when cross-border processing occurs and rules for determining the leading supervisory body and the main organisational unit within the meaning of the GDPR, when such cross-border processing takes place.

6. STOCKTAKING

6.1. **Sensitive data.** The Company identifies cases in which it processes or can process sensitive data (special data and criminal data) and keeps dedicated mechanisms in place to ensure compliance with provisions on sensitive data processing. If cases of sensitive data processing are identified, the Company follows the rules adopted in this respect.

6.2. **Unidentified data.** The Company identifies cases in which it processes or might process unidentified data and maintains mechanisms to facilitate the exercising of the rights of unidentified data subjects.

6.3. **Profiling.** The Company identifies cases in which profiling of the processed data is performed and maintains mechanisms which ensure compliance of this process with the law. In events when cases of profiling and automated decision-making are identified, the Company complies with the adopted rules in this respect.

6.4. **Joint controlling.** The Company identifies cases of joint controlling of data and proceeds in this respect in accordance with the adopted rules.

7. RECORD OF DATA PROCESSING ACTIVITIES

7.1. The Record is a form of documenting data processing activities, acts as a data processing map and is one of the key elements enabling the implementation of the fundamental principle on which the entire personal data protection system is based, i.e. the accountability principle.

7.2. The Company maintains a Record of Data Processing Activities in which it reviews and monitors the manner in which it uses personal data.

7.3. The Record is one of the basic tools enabling the Company to settle most of its data protection obligations.

7.4. In the Record, for each data processing activity which the Company has identified as a separate one for the needs of the Register, the Company records at least: (i) the name of the activity, (ii) the purpose of the processing, (iii) a description of the category of data subjects (iv) description of the data categories, (v) description of the categories of data recipients (including processors), (viii) information about a transfer outside the EU/EEA; (ix) a general description of the technical and organisational data protection measures.

8. GROUNDS FOR PROCESSING

8.1. The Company determines the legal grounds for data processing for individual processing activities.

8.2. The Company will define the general ground (consent, contract, legal obligation, vital interests, legitimate purpose of the Company) in a legible manner when it is needed. For example, in the case of consent, indicating its scope when the ground is a right – pointing to a specific provision and other documents, e.g. contract, vital interests – indicating the categories of events in which they apply, legitimate purpose – pointing to a specific goal, e.g. own marketing, pursuing claims.

8.3. The Company implements methods of managing consents, allowing for registration and verification of the consent of a person to process his/her specific data for a specific purpose, consent to remote communication (email, telephone, text messages) and registration of refusal of consent, withdrawal of consent and similar activities (objection, limitation, etc.).

8.4. The head of the Company's organisational unit is obliged to know the legal basis on which the unit he/she heads performs specific activities of processing personal data. If the legitimate interest of the Company is the ground for processing, the head of the unit is required to know the specific interest of the Company associated with the processing

9. MANNER OF HANDLING RIGHTS OF INDIVIDUALS AND INFORMATION OBLIGATIONS

9.1. The Company strives to ensure that the information provided and communication with the people whose data it processes is clear and has the right style.

9.2. The Company makes it easier for people whose data it processes to exercise their rights through various activities, including: posting information or (reference) links on the Company's website to information about the rights of individuals, the manners in which they are used in the Company, including identification requirements, methods of contact with the Company for this purpose, a possible price list of "additional" requests, etc.

9.3. The Company strives to ensure keeping legal deadlines for the performance of obligations towards the persons whose data it processes.

9.4. The Company implements adequate methods of identification and authentication of subjects whose data are processed for the purposes of exercising rights of individuals and information obligations.

9.5. In order to allow for exercising the rights of individuals, the Company provides for procedures and mechanisms to identify the data of specific subjects processed by the Company, integrate these data, introduce changes to them and delete them in an integrated manner,

9.6. The Company documents the handling of information obligations, notifications and requests of data subjects whose data it processes.

10. INFORMATION OBLIGATIONS

10.1. The Company defines lawful and effective means of performing information obligations.

10.2. The Company informs the data subject about extending the deadline for considering the request of that subject over one month.

10.3. The Company informs the data subject about the processing of its data when collecting data from that subject.

10.4. The Company informs the data subject about the processing of its data when collecting data about that data subject indirectly from it:

- **a.** within a reasonable time after obtaining personal data − at the latest within one month − taking into account the specific circumstances of the processing of personal data;
- **b.** if personal data are to be used for communication with the data subject − at the latest at the first such communication with the data subject; or
- **c.** if it is planned to disclose personal data to another recipient − at the latest at their first disclosure.

10.5. The Company defines the method of informing data subjects about the processing of unidentified data, where it is possible (e.g. a plate about the area being covered by video surveillance).

10.6. The Company informs the data subject about the planned change of the purpose of data processing.

10.7. The Company informs the data subject before a limitation of processing is revoked.

10.8. The Company informs the recipients of data about rectification, deletion or limitation of data processing (unless it will require a disproportionately large effort or will be impossible).

10.9. The Company informs the data subject about the right to object to the processing of data at the latest at the first contact with that person.

10.10. The Company informs the data subject without undue delay about the breach of personal data protection, if it may cause a high risk of violating the rights or freedoms of that data subject.

11. REQUESTS OF DATA SUBJECTS

11.1. **Third party rights.** By exercising third party rights of the data subjects, the Company introduces procedural guarantees to protect the rights and freedoms of these third parties. In particular, when reliable information is received that the execution of a data subject's request for a copy of the data or the right to portability of data may adversely affect the rights and freedoms of other data subjects (e.g. rights related to the protection of other people's data, intellectual property rights, trade secrets, personal rights, etc.), the Company may ask the person making the request to clarify doubts or take other lawful steps, including refusal to satisfy the claim.

11.2. **Not processing.** The Company informs a person that it does not process data concerning it, if such a person has made a request to be provided with such information.

11.3. **Refusal.** The Company informs the person who made the request within one month of receipt of the request about refusing to accept the request and about the rights of the person related to it.

11.4. **Access to data.** At the request of the data subject regarding access to its data, the Company informs the subject whether it processes its data and informs the person about the details of processing, in accordance with Article 15 of the GDPR (the scope corresponds to the information obligation upon data collection), and also provides the data subject making such a request with access to data concerning it. Access to the data may be provided by way of issuing a copy of the data, with the proviso that the Company will not recognise the copy of the data released in the exercise of the right of access data as the first free copy of data for the purposes of charging fees for copies of data.

11.5. **Copies of data.** At the request of the subject whose data is processed by the Company, the Company issues a copy of its data to that data subject and records the fact that the first copy of the data was issued. The Company introduces and maintains a price list for copies of data, in accordance with which it charges fees for subsequent copies of data. The price of a copy of the data is calculated on the basis of the estimated unit cost of servicing the request to issue a copy of the data.

11.6. **Correction of data.** The Company corrects incorrect data upon a justified request of the data subject who makes such a request. The Company has the right to refuse to correct the data if the data subject fails to demonstrate any irregularities in the data, the rectification of which is demanded. The Company informs each recipient to whom personal data have been disclosed about the rectification of the data, unless it proves impossible or would require a disproportionate effort. The Company informs the subject of the corrected data about those recipients, upon the request of the data subject.

11.7. **Completion of data.** The Company completes and updates data at the request of the data subject. The Company has the right to refuse to complete the data, if the completion would be incompatible with the purposes of data processing (e.g. the Company cannot process data, the processing of which is demanded by the data subject if they are unnecessary for the purpose of processing). The Company may rely on a statement of the data subject regarding the data to be completed, unless this is insufficient in the light of the procedures adopted by the Company (e.g. regarding obtaining such data), the law or when there are grounds to consider the statement unreliable.

11.8. **Deletion of data.** At the request of the data subject, the Company deletes data when:

- **a.** the data are not necessary for the purposes for which they were collected or otherwise processed,
- **b.** the consent to their processing has been withdrawn, and there is no other legal ground for processing,
- **c.** the data subject has effectively opposed the processing of these data,
- **d.** the data were processed unlawfully,
- **e.** the necessity to delete data results from a legal obligation,
- **f.** the request applies to a child's data collected on the basis of consent to provide information society services offered directly to a child (e.g. the child's profile on a social network, participation in a competition on the website).

The Company determines the manner of handling the right to delete data in such a way as to ensure effective implementation of this right, while respecting all data protection principles, including security, as well as verifying that no exceptions referred to in Article 17 (3) of the GDPR apply.

If the removed data have been made public by the Company, the Company undertakes reasonable actions, including technical measures, to inform other administrators processing these personal data, about the need to delete the data and access to those data.

In the case of data deletion, the Company informs the data subject about the recipients of the data at the request of that data subject.

11.9. **Limitation of processing.** The Company limits data processing at the request of the data subject when:

a. the data subject questions the correctness of the data – for a period allowing to verify their correctness,
b. the processing is unlawful and the data subject opposes the removal of personal data, requesting instead that their use be limited,
c. The Company no longer needs the personal data, however it is needed by the data subject to determine, assert or defend claims,
d. the data subject has objected to the processing for reasons related to its special situation – until it is determined whether the Company has legally justified grounds overriding the grounds of objection.

During the processing restriction, the Company stores data but does not process it (does not use it, does not transmit it) without the consent of the data subject, unless to establish, investigate or defend claims, or to protect the rights of another natural or legal person, or because of important public interest considerations.

The Company informs the data subject before revoking the processing limit.
In the case of limiting the processing of data, the Company informs the data subject about the recipients of the data at the request of that data subject.

11.10. Data portability. At the request of the data subject, the Company issues, in a structured, commonly used machine-readable format or transfers to another entity, **if** possible, data about that data subject which it provided to the Company, processed in the Company's IT systems based on the consent of that data subject or for the purpose of conclusion or performance of an agreement concluded with that data subject.

11.11. Objection in a special situation. If a data subject submits an objection motivated by its special situation and objects to the processing of its data, and the data are processed by the Company based on the legitimate interest of the Company or the task entrusted to the Company under a public interest, the Company will **take into account** the objection unless the Company has valid legally justified grounds to process the data, overriding the interests, rights and freedoms of the objecting data subject, or grounds for establishing, perusing or defending claims.

11.12. for scientific, historical or statistical purposes. If the Company conducts scientific research, historical research or processes data for statistical purposes, the person may submit an objection motivated by its special situation motivation against such processing. The Company will take into account such an objection, unless the processing is necessary to perform the task carried out in a public interest.

11.13. Objection against direct marketing. If a data subject objects to the processing of its data by the Company for direct marketing purposes (including **possibly** profiling), the Company will take into account the objection and will discontinue such processing.

11.14. The right to human intervention with automatic processing. If the Company processes data automatically, including in particular performs profiling of data subjects, and consequently takes decisions with respect to a data subject which causes legal effects or significantly affects the **data subject**, the Company provides for the opportunity to introduce human intervention and human-made decisions on the part of the Company, unless such an automatic decision (i) is necessary for the conclusion or performance of the contract between the appealing data subject and the Company; or (ii) is expressly permitted by law; or (iii) is based on express consent of the appealing data subject.

12. MINIMALISATION

The Company strives to ensure minimisation of data processing in terms of: (i) the adequacy of the data for the purposes (amount of data and scope of processing), (ii) data access, (iii) data storage time.

12.1. Minimising the scope. The Company has verified the scope of the collected data, the scope of their processing and the amount of data processed in terms of adequacy for purposes of processing as part of its procedures to implement the GDPR. The Company reviews the amount of data processed and the scope of its processing periodically, at least once a year. The Company performs verification of changes in the amount and scope of data processing under change management procedures (privacy by design).

12.2. Minimising access. The Company applies restrictions on access to personal data: legal (confidentiality obligations, authorisation limits), physical (access zones, locking of premises) and logical (authorisation restrictions regarding systems processing personal data and network

resources in which personal data reside). The Company applies physical access control. The Company updates the access rights when changing the composition of staff and upon changes in the roles of persons, as well as changes in the processors. The Company periodically reviews the established system users and updates them at least once a year. Detailed rules for physical and logical access control are included in the procedures regarding technical organisational measures to ensure the security of the data processed, issued as part of the application of the Policy.

12.3. Minimising time. The Company implements life-cycle data protection mechanisms in the Company, including verification of the further suitability of the data in relation to the dates and control points indicated in the Register. Data, whose scope of use is limited with the passage of time, are removed from the Company's production systems, as well as from handheld and main files. Such data may be archived and be stored on back-up systems and information processed by the Company. Procedures for archiving and using archives, creating and using backup copies take into account the requirements of controlling the life cycle of data, including the requirements for data deletion.

13. SECURITY

The Company ensures a level of data security corresponding to the risk of violation of the rights and freedoms of individuals as a result of the processing of personal data by the Company.

13.1. Risk analysis and adequacy of security measures. The Company carries out and documents the adequacy analysis of its personal data security measures. For this purpose:

a. The Company provides for an appropriate state of knowledge on information security, cybersecurity and operation continuity − either internally or with the support of specialised entities.

b. The Company categorises data and processing activities in terms of the risk they present.

c. The Company conducts analyses of the risk of violation of the rights or freedoms of individuals for data processing activities or categories of data. The Company analyses possible situations and scenarios of personal data breaches taking into account the nature, scope, context and purposes of processing, the risk of violation of the rights or freedoms of individuals with varying likelihood of occurrence and the severity of the threat.

d. The Company determines the organisational and technical security measures which can be applied and assesses the cost of their implementation. The Company determines the suitability of and applies such measures and approaches as:

(i) pseudonymisation,

(ii) encryption of personal data,

(iii) other cyber security measures consisting of the ability to continually ensure the confidentiality, integrity, availability and resilience of processing systems and services,

(iv) measures used to ensure operation continuity and to prevent the consequences of disasters, i.e. the ability to quickly restore the accessibility of personal data and access to them in the event of a physical or technical incident.

13.2. Impact assessment for data protection. The Company evaluates the effects of planned processing operations for the protection of personal data where, in accordance with the risk analysis, the risk of violating the rights and freedoms of persons is high. The Company uses the impact assessment methodology adopted at the Company.

13.3. Security measures. The Company applies security measures established as part of risk analyses and the adequacy of security measures and impact assessments for data protection. Personal data security measures are part of information security and cyber security measures in the Company and are described in more detail in the procedures adopted by the Company for these areas.

13.4. Reporting breaches. The Company uses procedures to identify, assess and report an identified data breach to the Data Protection Authority within 72 hours of the establishment of the breach.

14. PROCESSOR

The Company has principles of selection and verification of data processing for the Company in place, designed to ensure that the processors provide sufficient guarantees to implement appropriate organisational and technical measures to ensure security, implementation of individual rights and other data protection obligations on the Company. The Company concludes data processing agreements which meet the requirements of the GDPR. The Company makes processors account for the use of sub-processors, as well as other requirements resulting from the Principles of entrusting personal data.

15. DATA EXPORT

The Company registers cases of data export, i.e. transmission of data outside the European Economic Area (EEA in 2017 = European Union, Iceland, Lichtenstein and Norway) in the Record. In order to avoid unauthorised data export, in particular in connection with the use of publicly available cloud services (shadow IT), the Company periodically verifies the behaviour of users and, where possible, makes equivalent solutions available in accordance with data protection law.

16. PRIVACY BY DESIGN

The Company manages the change affecting privacy in such a way as to enable adequate security of personal data and minimise their processing.
To this end, the principles of project and investment management by the Company refer to the principles of personal data security and minimisation, requiring an impact assessment on privacy and data protection, consideration and design of security and minimisation of data processing from the beginning of the project or investment.

17. FINAL PROVISIONS

The provisions of the Policy may be changed by way of a resolution adopted by the Management Board.

The Policy enters into force on 28 May 2018.

BPH - BRITISH PUBLISHING HOUSE LTD.
72 Great Suffolk Street, London, UK
Tel.: +44 20 81 33 44 88
Email: office@britishpedia.com