Schedule 8 - Draft Data Processing Agreement

KB and enter the Counterparty's name

Contents

ARTICLE PAGE

DATA PROCESSING AGREEMENT ARBIT-2022

THE UNDERSIGNED,

(1) Koninklijke Bibliotheek [the National Library of the Netherlands], having its statutory registered office at Prins Willem-Alexanderhof 5 in (2595 BE) The Hague, the Netherlands (hereinafter referred to as the **'the Contracting Authority'**);

(2) [Full name and legal structure of the Counterparty, which will be acting as a data processor,, having its statutory registered office in Address and country and (hereinafter referred to as **'the Counterparty'**);

hereinafter jointly referred to as the '**Parties**' and severally as a '**Party**';

WHEREAS:

- In so far as the Counterparty processes Personal Data for the Contracting Authority in the context of the Contract, the Contracting Authority qualifies as a Controller for the Processing of Personal Data and the Counterparty as a Processor;
- The Parties to this Data Processing Agreement, as referred to in Article 28, paragraph 3 of the Regulation, wish to record their agreements on the Processing of Personal Data by the Counterparty.

AGREE AS FOLLOWS:

Article 1. Definitions

Certain terms in this Data Processing Agreement are written with initial capitals. These terms are defined in the ARBIT-2022 or the Regulation, on the understanding that the definitions of a number of terms are geared to the Data Processing Agreement. In addition thereto, the following terms are thus defined below for the purposes of this Data Processing Agreement, regardless of whether they are used in the singular or plural or as verbs or nouns:

1.1 ARBIT-2022: General Government Terms and Conditions for IT Contracts 2022.

1.2 Data Subject: the person whom the Personal Data concerns.

1.3 EEA: the European Economic Area, comprising all EU countries in addition to Liechtenstein, Norway and Iceland.

1.4 Personal Data Breach: a breach in security that leads to the accidental or unlawful destruction, loss, change or unauthorised disclosure of, or unauthorised access to, data that has been transferred, stored or Processed in any other way.

1.5 Recipient: a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or member state law are not regarded as Recipients; the Processing of that data by those public authorities takes place in compliance with the data protection rules applicable to the purposes of the processing.

1.6 Contract: the agreement between the Contracting Authority and the Counterparty [title], reference number **581493**.

1.7 Personal Data: any data concerning an identified or identifiable natural person that is Processed by the Counterparty for the Contracting Authority in the context of the Contract.

1.8 Supervisory Authority: an independent public authority which is established by a member state pursuant to Article 51 of the Regulation.

1.9 Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council 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).

1.10 Processor: a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.11 Data Processing Agreement: this agreement including its recitals and the accompanying Annexes.

1.12 Processing: any operation or any set of operations concerning Personal Data or any set of Personal Data, carried out in the context of the Contract via automated or manual procedures, including in any case the collection, recording, organisation, structuring, storage, updating or modification, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

1.13 Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or member state law, the Controller or the specific criteria for its nomination may be provided for by Union or member state law.

Article 2. Object of this Data Processing Agreement

2.1 This Data Processing Agreement governs Processing by the Counterparty in the context of the Contract and is inextricably linked to the Contract.

2.2 The nature and purpose of the Processing, the type of Personal Data and the categories of Personal Data, Data Subjects and Recipients are set out in Annex 1.

2.3 The Counterparty guarantees that the appropriate technical and organisational measures will be taken, in order to ensure that Processing complies with the requirements of the Regulation and that the rights of the Data Subject(s) are protected.

2.4 The Counterparty guarantees compliance with the requirements of the applicable legislation relating to the Processing.

Article 3. Entry into force and term

3.1 This Data Processing Agreement enters into force as soon as it has been signed by both Parties.

3.2 This Data Processing Agreement terminates after and in so far as the Counterparty has erased or returned all Personal Data and has deleted existing copies in accordance with article 10 of this Data Processing Agreement.

3.3 Early termination of this Data Processing Agreement is not possible.

Article 4. Scope of the Counterparty's Processing competence

4.1 The Counterparty will Process Personal Data only for, and on the basis of written instructions from, the Contracting Authority, unless the Counterparty is required by a statutory regulation to carry out Processing. In that case the Counterparty will notify the Contracting Authority of such a statutory regulation prior to the Processing, unless that statutory regulation prohibits such notification on important grounds of public interest.

4.2 The Counterparty has no control over the purpose or means of the Processing within the meaning of the Regulation.

Article 5. Security of the Processing

5.1 Without prejudice to article 2.3 of this Data Processing Agreement, the Counterparty will implement the technical and organisational security measures described in Annex 3.

5.2 The Parties recognise that guaranteeing an appropriate level of security may require additional security measures to be implemented on an ongoing basis. The Counterparty guarantees an appropriate level of security having regard to the risks entailed.

5.3 At the express written request of the Contracting Authority, the Counterparty will adopt additional measures to ensure the security of the Personal Data.

5.4 The Counterparty will not Process any Personal Data outside the EEA unless it has obtained express written consent from the Contracting Authority to do so, subject to further conditions if necessary, and barring statutory obligations to the contrary.

5.5 As soon as the Counterparty becomes aware of any illegal or unauthorised Processing of Personal Data or breaches of the security measures referred to paragraphs 1 and 2, it will inform the Contracting Authority without unreasonable delay.

5.6 The Counterparty will assist the Contracting Authority in ensuring compliance with the obligations under Articles 32 to 36 inclusive of the Regulation.

Article 6. Duty of Confidentiality of the Counterparty's Staff

6.1 The Personal Data is confidential as referred to in article 17.1 of the ARBIT-2022.

6.2 The Counterparty guarantees that its Staff have undertaken to observe the duty of secrecy referred to in article 17.2 of the ARBIT-2022.

Article 7. Subprocessor

If the Counterparty, with due regard for the provisions of article 23 of the ARBIT-2022, engages another Processor to carry out processing activities for the Contracting Authority, the other Processor must be bound by an agreement imposing the same data protection obligations as those imposed by this Data Processing Agreement.

Article 8. Assistance concerning rights of Data Subjects

8.1 Taking into account the nature of the processing, the Counterparty will assist the Contracting Authority by means of appropriate technical and organisational measures, in so far as this is possible, in the fulfilment of the Contracting Authority's obligation to respond to requests for exercising the Data Subject's rights laid down in chapter III of the Regulation.

8.2 Each of the Parties will bear any costs they incur in connection with paragraph 1.

Article 9. Personal Data Breach

9.1 The Counterparty will inform the Contracting Authority, without unreasonable delay, as soon as it becomes aware of any Personal Data Breach, in accordance with the agreements set out in Annex 4.

9.2 After reporting an incident as described in paragraph 1, the Counterparty will also inform the Contracting Authority of developments relating to the Personal Data Breach.

9.3 Each of the Parties will bear any costs they incur in connection with reporting incidents to the competent Supervisory Authority and the Data Subject.

Article 10. Return or erasure of Personal Data

10.1 Once the Contract expires or earlier as agreed the Counterparty will ensure that it erases all the Personal Data or returns it to the Contracting Authority, whichever the Contracting Authority prefers, and deletes existing copies, unless statutory regulations require the storage of the Personal Data.
If the Counterparty is to erase and/or delete copies, it will inform the Contracting Authority as soon as it has done so.

10.2 The Parties may agree retention periods for separate Personal Data or categories of Personal Data. Once the agreed retention period has expired, the Counterparty will ensure the erasure or return and the deletion of copies of the Personal Data concerned unless statutory regulations require the storage of the Personal Data.

10.3 The Counterparty will [erase or return] the Personal Data within [number] [days/weeks] following the expiry of the Contract or earlier as agreed.

10.4 The Personal Data will be returned in the format and manner stipulated by the Contracting Authority.

Article 11. Obligation to supply information and audit obligation

In order to demonstrate that the obligations under this Data Processing Agreement have been and are being fulfilled by the Counterparty, the Contracting Authority may, in accordance with article 5 of the ARBIT-2022, request information or have an audit performed.

THUS AGREED AND SIGNED AS TWO ORIGINALS.

The Contracting Authority Koninklijke Bibliotheek	Counterparty Counterparty's Name
_____	_____
Name: Eva de Jong authorised to sign	Name: Name of person
Position: Board member with the portfolio Business management	Position: position

KB Privacy lawyer's initials	KB Owner's initials
_____	_____

Annex 1 – Personal Data and Processing Activities

This Annex constitutes part of the Data Processing Agreement, the Contracting Authority needs to complete it.

1. Subject: the Processing of Personal Data as stipulated in greater detail in this Data Processing Agreement and the Agreement A brief description of the service(s) which the Counterparty is to provide

2. Categories of Data Subjects: these are people whose Personal Data is Processed by the Counterparty.Indicate who may be deemed to be Data Subjects in relation to the service. Indicate who may be deemed to be Data Subjects in relation to the service.

[NB. TICK WHAT IS APPLICABLE AND DELETE WHAT IS NOT.
- *employees;*
- *job applicants;*
- *self-employed workers;*
- *business associates;*
- *network partners;*
- *clients;*
- *members;*
- *users of services;*
- *others, namely....*

3. The Personal Data (or categories thereof) to be Processed: the Counterparty will Process the following Personal Data (or categories thereof) at the The Contracting Authority's behest. Enter categories of Personal Data See the examples below and delete if not applicable.

[NB. TICK WHAT IS APPLICABLE AND DELETE WHAT IS NOT.
- *name, address, postcode and place of residence;*
- *title;*
- *gender;*
- *telephone number;*
- *email address;*
- *date of birth;*
- *profession/ trade*
- *nationality;*
- *citizen service number;*
- *financial details such as bank account number, payment and transaction details, donations and other financial data; [Fill in what is applicable.]*
- *customer, membership or card number;*
- *type of membership*
- *loan details, reading details (e.g. bookmark), details of use;[Fill in what is applicable.]*
- *social media account and data sourced from social profiles (Facebook or Twitter account and so forth);*
- *IT information (IP address, MAC ID, and device, details on use and location and cookie details);*
- *other, namely.....*

4. Retention period: how long the Counterparty stores Personal Data, or mention the criteria which are used to determine the retention period.
Cite or mention the retention period.

5. Purpose: Any Personal Data will be processed for the purposes of providing the services mentioned in the Agreement and this Data Processing Agreement.
Purposes of describing the Processing

KB Privacy lawyer's initials

_____

Annex 2 – List of approved Sub-processors and Transfers outside the EEA

This Annex constitutes part of the Data Processing Agreement, the Contracting Authority or the Counterparty needs to complete it.

Approved Sub-processors:

The Contracting Authority has granted the The Counterparty specific consent to engage the Sub-processor(s) mentioned below.

Name of Sub-processor whom the Counterparty has engaged	**Country in which Sub-processor has Its Registered Office**	**Type of Activity**	**Processing Country (including data storage)**
[Sub-processor's name and legal structure]	[address and country]	[e.g. hosting, supplier of content and customer support]	

KB Privacy lawyer's initials

_____

Annex 3 – Security measures

This Annex constitutes part of the Data Processing Agreement, the Counterparty needs to complete it, and both Parties are required to initial it.

The Counterparty will supply this information and the Contracting Authority will assess it in the light of its data security policy.

The security measures which the Counterparty has adopted and which apply in relation to the activities referred to in the Agreement are set out below.

DESCRIPTION OF THE SECURITY MEASURES TO BE ADOPTED BY THE COUNTERPARTY

A description of the security measures to be adopted by the Counterparty

[NB. TICK WHAT IS APPLICABLE AND SUPPLEMENT IT.

- *Anonymization (including test data)*
- *Application white-listing*
- *Personal Data access audit log*
- *Backups*
- *Off-site backups*
- *Secure remote access*
- *CERT and CSIRT*
- *Security and privacy certification*
- *Cybersecurity and privacy awareness training*
- *Data validation*
- *Data destruction in accordance with official standards*
- *DDoS protection*
- *Encryption of data at rest*
- *Encryption of data in transit*
- *Firewalls*
- *Physical access security*
- *Automated or other erasure of data after the retention period*
- *Fictional test data*
- *IP white-listing*
- *Pen testing (and reports capable of being presented)*
- *Role-based access control*
- *Clear-screen policy*
- *Security monitoring and SIEM*
- *Single sign-on*
- *SOC 2 Type II reports capable of being presented*
- *Two-factor authentication*
- *Update and patch policy*
- *Other, namely, ...*

KB (deputy) CISO's initials

_____

Annex 4 – Reporting a security breach

This Annex constitutes part of the Data Processing Agreement, the Counterparty needs to complete it.

To report a security breach referred to in Article 7 the Counterparty will contact the Contracting Authority's **Computer Security Incident Response Team** (KB CSIRT).

Accessible: Mondays to Fridays from 6 am to 11 pm
Saturdays and Sundays from 10 am to 11 pm

Telephone number: +31 (0)70 314 0314
Email address: csirt@kb.nl

Using the data mentioned below, the Contracting Authority may contact the Counterparty for the purposes of communication concerning a security breach referred to in Article 7.

Name	**Position / Role**	**Email address**	**Telephone Number**	**Contact Period**
[full name[	[e.g. FG, CISO, CERT]			

A report of a Security Breach referred to in Article 7 must at any rate contain the following details:

a. the nature of the Security Breach, where possible mentioning the categories and estimated number of Data Subjects and amount of Personal Data involved;
b. whether the Personal Data is encrypted, anonymised or otherwise rendered incomprehensible;
c. the name and contact details of the data protection officer or any other contact person from whom additional information may be obtained;
d. the likely consequences of the Security Breach; and
e. the measures which the Counterparty has taken or proposes to take to tackle the Security Breach, including, as the case may be, measures to limit any potential adverse effects thereof.

KB Privacy lawyer's initials

_____