

ASML Binding Corporate Rules for Business Partner Data (BCR for Business Partner Data)

(Binding Corporate Rules for the transfer of personal data outside the EEA under Article 47 GDPR)

Introduction

ASML has committed itself to the protection of personal data it processes of its employees, Business Partners in its [Code of Conduct](#), which refers to the Privacy Policy. The ASML Privacy Policy includes these BCR and its sub-policies.

These BCR for Business Partner Data constitutes Binding Corporate Rules for the transfer of personal data to a third country outside the EEA under Article 47 GDPR and is legally binding and shall apply to and be enforced by ASML and its Group Companies, including Employees.

For the BCR applicable to employee data, please refer to the *BCR for Employee Data*.

Capitalized terms not defined in Annex 1 will have the meaning given to them in the GDPR.

Article 1 – Scope, Applicability and Implementation

Scope	1.1	These BCR for Business Partner Data (BCR) address the Processing of Personal Data of Business Partners and other Individuals (Personal Data) by ASML that are: (i) subject to EEA Data Protection Laws (or were subject to EEA Data Protection Laws prior to the Transfer to a Group Company), and (ii) are transferred to a Group Company in a Third Country.
Applicability of law and these BCR for Business Partner Data	1.2	Individuals will keep any rights and remedies they may have under applicable local law. For the avoidance of doubt: (i) where applicable local law provides more protection than these BCR for Business Partner Data, local law will apply in addition to these BCR for Business Partner Data and (ii) where these BCR for Business Partner Data provide more protection than applicable local law or provide additional safeguards, rights or remedies for Individuals, these BCR for Business Partner Data will apply in addition to applicable local law.
Sub-policies and notices	1.3	ASML may supplement these BCR for Business Partner Data through sub-policies, guidelines or notices that are consistent with these BCR for Business Partner Data.
Accountability for compliance	1.4	These BCR for Business Partner Data, including any sub-policies or guidelines, are legally binding and shall apply to and be enforced by ASML and its Group Companies, including Employees. The responsible executives and the Controllers within the ASML Group will be accountable for compliance with these BCR for Business Partner Data. The Board of Management will ensure compliance with these BCR for Business Partner Data throughout ASML and its Group Companies.
Effective Date	1.5	These BCR for Business Partner Data have been adopted by the Board of Management. They have entered into force as of 4 December 2025 (Effective Date). They will be published on the ASML website and ASML intranet. They will further be made available to Individuals upon request.
Conflicts	1.6	In case of conflict between provisions of these BCR for Business Partner Data and other ASML policies, guidelines and notices that exist on or after the Effective Date, the provisions of these BCR for Business Partner Data will prevail.

Implementation	1.7	These BCR for Business Partner Data will be implemented in the ASML organization based on the timeframes specified in Article 22.
Role of ASML Netherlands	1.8	ASML Holding has tasked ASML Netherlands with the coordination and implementation of these BCR for Business Partner Data.
Interpretation	1.9	In these BCR for Business Partner Data, “may” means a choice, “will” means a rule and “shall” means an obligation.

Article 2 – Purposes for Processing Personal Data

Lawful Processing	2.1	<p>Personal Data shall be Processed lawfully. Lawful Processing means that ASML will not Process Personal Data, unless one of the following conditions applies:</p> <ul style="list-style-type: none"> (i) ASML needs to Process the Personal Data to: <ul style="list-style-type: none"> (a) perform, or take steps with a view to enter into, a contract with the relevant Individual; (b) comply with a legal obligation to which ASML is subject; (c) protect the vital interests of the Individual; (ii) ASML needs to carry out such Processing to pursue ASML’s legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Individual concerned; or (iii) the Individual concerned has consented to the Processing, by providing a freely given, specific, informed and unambiguous indication of the Individual’s wishes by a clear affirmative action; (iv) In circumstances permitted by EEA Laws. <p>ASML will not use Personal Data for new purposes without following our internal procedures to verify that such Processing can take place lawfully.</p>
Legitimate Business Purposes	2.2	<p>The Processing of Personal Data for one of the following purposes (Business Purposes) in the context of ASML’s business activities as a manufacturer and supplier of chip making equipment and the provider of related services, can generally be based on one of the main legal bases set out in Article 2.1, but remains subject to any applicable requirements and restrictions under EEA Law:</p> <ul style="list-style-type: none"> (i) Assessment and acceptance of a Business Partner, conclusion and execution of agreements with a Business Partner. This purpose includes Processing of Personal Data that is necessary in connection with the assessment and acceptance of Business Partners including confirming and verifying the identity of relevant individuals (this may involve the use of a credit reference agency or other Third Parties) and conducting due diligence (e.g. continuity risk assessments), screening (e.g. against publicly available government and/or law enforcement agency sanctions list and for access to ASML’s premises or systems). This activity also includes the Processing of Personal Data in connection with the execution of agreements, including the delivery of Customer Services and obtaining visa’s, permits and technology export licenses, and to record and financially settle delivered services, products and materials to and from ASML; (ii) Development and improvement of products and/or services. This purpose includes Processing of Personal Data that is necessary for the development and improvement of ASML products and/or services (including Customer Services), research and development;

- (iii) **Relationship management and marketing.** This purpose includes activities such as maintaining and promoting contact with Business Partners, account and relation management, service, recalls and the development, execution and analysis of market surveys and marketing strategies;
- (iv) **Business process execution, internal management and management reporting.** This purpose includes the management of company assets, conducting audits and (internal) investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes managing mergers, acquisitions and divestitures, and Processing Personal Data for management reporting and analysis, archive and insurance purposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution;
- (v) **Health, safety, security and integrity.** This purpose includes the protection of the interests of ASML and its Employees and Business Partners, and activities such as those involving safety and health, the protection of ASML, Employee and Business Partner assets, and the authentication of Business Partner status and access rights;
- (vi) **Compliance with law.** This purpose addresses the Processing of Personal Data as necessary for compliance and the performance of a task carried out to comply with or authorized by law including the disclosure of Personal Data to government institutions or supervisory authorities in relation thereto or
- (vii) **Protection of the vital interests of Individuals.** This is where Processing is necessary to protect the vital interests of an Individual.

Where there is a question whether a Processing of Personal Data can be based on a Business Purpose, the appropriate Privacy Officer will be consulted before the Processing takes place.

Consent

- 2.3 If a legal ground as set forth in article 2.1(i),(ii) and (iv) does not exist or if EEA Law so requires ASML shall (also) seek consent from the Individual for the Processing.

Subject to Article 2.4, where Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he or she will be deemed to have provided consent to the Processing which is necessary for the performance requested by the Individual.

When seeking Individual consent for Processing, ASML shall inform the Individual:

- (i) of the purposes of the Processing for which consent is requested;
- (ii) which Group Company is responsible for the Processing;
- (iii) of other relevant information (e.g., the nature and categories of the Processed Personal Data, the categories of Third Parties to which the Personal Data are disclosed (if any) and how Individuals can exercise their rights); and
- (iv) that the Individual may deny or withdraw consent at any time. Upon withdrawal of consent, ASML will discontinue the Processing. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its withdrawal; and (ii) the lawfulness of Processing of the relevant Personal Data after withdrawal, for other Processing Purposes not based on consent.

Consent under GDPR

- 2.4 ASML will ensure that any consent for Personal Data collected will meet the criteria of Article 7 of the GDPR.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

- 3.1 Personal Data may be Processed for a purpose other than the Business Purpose(s) for which the Personal Data was originally collected, only if the additional purpose is compatible with the relevant Business Purpose(s), taking into account the link between the original and additional purpose, the context in which the Personal Data is collected, the nature of the relevant Personal Data and the implementation of appropriate safeguards set out below (**Secondary Purpose**). When assessing if Personal Data can be Processed for a Secondary Purpose, the appropriate Privacy Officer will be consulted.

Depending on the sensitivity of the relevant Personal Data and the possible consequences for the Individual, the Processing of Personal Data for the Secondary Purpose may require additional safeguarding measures such as:

- (i) limiting access to the Personal Data;
- (ii) imposing additional confidentiality requirements;
- (iii) taking additional security measures;
- (iv) providing an opportunity to object to the Processing (when basing the Secondary Purpose on any other legal ground than the Individual's consent); or
- (v) obtaining an Individual's consent in accordance with Articles 2.3 and 2.4 or Article 4.4 (if applicable).

Examples of Uses for Secondary Purposes

- 3.2 To the extent not already covered in Article 2.1, and subject to the compatibility assessment referred to in Article 3.1, below are a number of examples of Processing for Secondary Purposes that may be permissible:
- (i) anonymization or pseudonymization of the Personal Data;
 - (ii) internal audits or investigations;
 - (iii) implementation of business controls and operational efficiency;
 - (iv) IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);
 - (v) for the purposes of public interest, scientific or historical research purposes or statistical purposes, including the archiving of the Personal Data for these purposes;
 - (vi) dispute resolution;
 - (vii) legal or business consulting; or
 - (viii) insurance purposes.

The Business Purposes and Secondary Purposes together constitute the **Processing Purposes**.

Article 4 – Purposes for Processing Special Categories of Data

Lawful Processing of Special Categories of Data

- 4.1 Special Categories of Data shall be Processed lawfully. Lawful Processing means that ASML will not Process Special Categories of Data, unless one of the following conditions apply:
- (i) Processing is required or allowed by EEA Law (e.g., for reasons of public interest, and for archiving, scientific or historical research purposes or statistical purposes);
 - (ii) Processing is necessary for the establishment, exercise or defence of a legal claim;

- (iii) Processing is necessary to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first;
- (iv) Special Categories of Data have manifestly been made public by the Individual (e.g. via ASML social media channels).

Specific purposes for Processing Special Categories of Data

4.2 Subject to Article 4.1, ASML shall Process Special Categories of Data only to the extent necessary to serve one or more of the purposes specified below or as provided by EEA Law.

- (i) **Racial or ethnic data:** in some countries photos and video images of Individuals qualify as racial or ethnic data. ASML may Process photos (e.g. a copy of a passport containing a photo) and video images for the protection of ASML and Employee assets, site access and security reasons, the identification and the authentication for compliance with financial regulatory laws, anti-money laundering and financing of terrorism laws of Business Partner status and access rights (including confirming and verifying the identity of relevant Individuals), demographic reporting under applicable anti-discrimination laws, for obtaining visas, permits and technology export licenses and to record decisions made in the course of business for future reference (e.g. when Individuals participate in video conferencing which is recorded).
- (ii) **Physical or mental health data:** insofar as necessary for the assessment and acceptance of a Business Partner and the execution of an agreement with a Business Partner.
- (iii) **Religion or philosophical beliefs:** accommodating specific products or services for a Business Partner, dietary requirements or religious holidays.

Consent, and the denial or withdrawal of consent for Processing Sensitive of Data

4.3 In addition to the specific purposes listed in Article 4.2 and the general conditions listed in Article 4.1, all categories of Special Categories of Data may be Processed if the Individual has given his or her explicit consent to the Processing thereof. If one of the conditions listed in Article 4.1 applies, ASML shall in addition seek consent if applicable law so requires. The information requirements set out in Article 2.3 through 2.4 will apply to the granting, denial or withdrawal of consent.

Use of Special Categories of Data for Secondary Purposes

4.4 Special Categories of Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3 and only if one of the conditions of Article 4.1 or Article 4.3 applies.

Criminal Data

4.5 Criminal Data may be collected, used or otherwise Processed only for one or more of the purposes specified below and on condition that the Processing (a) shall be carried out under the control of official authority of a country in the EEA, or (b) is authorized by EEA Law:

- (i) assessing an application by an Individual to make a decision about the Individual or provide a service to the Individual;
- (ii) protecting the interests of ASML, its Employees, customers, suppliers or business partners with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against ASML or its employees, customers, suppliers or business partners.

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	ASML shall limit the Processing of Personal Data to the Personal Data that are reasonably adequate and necessary for and relevant to the applicable Processing Purpose. ASML shall take reasonable steps to delete or otherwise destroy Personal Data that are not required for the applicable Processing Purpose.
Storage period	5.2	<p>ASML specifies – e.g. in a policy, statement, records retention schedule or in new systems via ‘privacy by design’ - a time period for which certain categories of Personal Data may be kept, which means not for longer than necessary for the applicable Processing Purpose.</p> <p>Upon the end of the storage period, the Personal Data shall be:</p> <ul style="list-style-type: none"> (i) securely deleted or destroyed; (ii) anonymized; or (iii) kept as necessary for litigation purposes or compliance with legal record keeping obligations.
Quality of Data	5.3	Personal Data will be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Processing Purpose. ASML shall take reasonable steps to rectify or erase Personal Data that is inaccurate without delay.
Accurate, complete and up-to-date Data	5.4	ASML may ask Individuals to inform ASML regarding any changes in their Personal Data and to keep their Personal Data accurate, complete and up-to-date. Individuals shall inform ASML regarding any changes in accordance with Article 7.

Article 6 – Individual Information Requirements

Information requirements	6.1	<p>At the time when Personal Data is obtained, or prior to Processing Personal Data for a Secondary Purpose, ASML shall inform Individuals through a privacy policy or privacy notice of the following:</p> <ul style="list-style-type: none"> (i) the nature and categories of Personal Data Processed; (ii) which Group Company or Group Companies are solely or jointly responsible for the Processing; (iii) the contact details of the relevant Privacy Officer or designated central point of contact for data privacy matters within ASML; (iv) the Processing Purposes for which their Personal Data are Processed; (v) the legal basis for the Processing of their Personal Data and, if the Processing is based on the legitimate interests of ASML, of the legitimate interests pursued by ASML; (vi) the categories of Third Parties to which the Personal Data are disclosed (if any); (vii) if applicable, the fact that Personal Data will be transferred to an international organization or a Third Party located in a Third Country, including the safeguards in place to protect the Personal Data; and (viii) to the extent applicable, any other relevant information, such as: <ul style="list-style-type: none"> a) the retention period of the Personal Data or the criteria to determine the retention period; b) the Individual's rights under these BCR and how these rights may be exercised, including the right to obtain compensation; c) the right to withdraw consent; d) the right to lodge a complaint to a Data Protection Authority or a competent court; e) whether an Individual is required to provide Personal Data;
---------------------------------	-----	---

- f) about existence of automated decision making, including profiling, and about the logic behind and envisaged consequences of this automated decision making; and
- g) if the Personal Data were not obtained from the Individual, the source from which the Personal Data originate.

Personal Data not obtained from the Individual

- 6.2 Where Personal Data have not been obtained directly from the Individual, ASML shall provide the Individual with the information as set out in Article 6.1:
- (i) within one month after the Personal Data are recorded in a ASML database;
 - (ii) at the time that the Personal Data are first used for a mailing, and at the latest within six months after the Personal Data are recorded in a ASML database; or
 - (iii) at the time that the Personal Data are first disclosed to a Third Party, and at the latest within six months after the Personal Data are recorded in an ASML database.

Exceptions

- 6.3 The requirements of Article 6.1 may be set aside if:
- (i) it is impossible or would involve a disproportionate effort to provide the information to Individuals;
 - (ii) it results in disproportionate costs;
 - (iii) the Individual already has this information; or
 - (iv) disclosure is expressly provided by EEA Law.

Article 7 – Individual Rights

Rights of Individuals

- 7.1 Every Individual has the right to access his or her Personal Data Processed by or on behalf of ASML. Where reasonably possible, the overview will contain information regarding the source, type, purpose, categories of recipients and envisaged retention period or criteria to determine such retention period of the relevant Personal Data.

If the Personal Data are incorrect, incomplete or not Processed in compliance with EEA Law or these BCR for Business Partner Data, the Individual may have his or her Personal Data rectified, deleted or their Processing restricted (as relevant).

In addition, the Individual may:

- (i) object to the Processing on the basis of compelling grounds related to his or her particular situation;
- (ii) object to receiving marketing communications on the basis of Article 9.5;
- (iii) be informed of the safeguards implemented by ASML to provide an adequate level of protection of Personal Data transferred to a Third Party located in a Third Country;
- (iv) restrict the Processing if he or she contests the accuracy of his or her Personal Data, or if the Individual objects to the Processing or does not agree to deletion of his or her Personal Data;
- (v) restrict the Processing if the Processing is unlawful and the Individual objects to the deletion of his or her Personal Data; and
- (vi) receive a machine-readable copy of his or her Personal Data and, where technically possible, to have ASML transmit his or her Personal Data to a Third Party directly. This right will only apply where the Processing is carried out by automated means and is based on consent as set forth in Articles 2.3 or 4.3, or based on a

contract.

Where the Individual objects to the Processing following this Article and this objection is justified, and ASML has no compelling legitimate grounds for the Processing that override the Individual's interests, the objected Processing will be ceased.

Procedure

- 7.2 The Individual shall send his or her request to the contact person or contact point indicated in the relevant privacy statement or notice. If no contact person or contact point is indicated, the Individual may send his or her request through the general contact section of the ASML website.

Prior to fulfilling the request of the Individual, ASML may require the Individual to:

- (i) If ASML Processes a large quantity of Personal Data relating to the Individual:
 - a. specify the categories of Personal Data to which he or she is seeking access;
 - b. specify, to the extent reasonably possible, the product line to which his request relates to determine where the Personal Data are likely to be stored;
 - c. where the request does not relate to data Processed in the context of a product line, specify, to the extent reasonably possible the circumstances in which ASML obtained the Personal Data;
- (ii) provide proof of his or her identity; and
- (iii) in the case of a request for rectification, deletion, or restriction specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with EEA Law or these BCR for Business Partner Data.

Response period

- 7.3 Within one month of ASML receiving the request, the contact person, contact point or Privacy Officer shall inform the Individual in writing either (i) of ASML's position with regard to the request and any action ASML has taken or will take in response or (ii) of the ultimate date on which he or she will be informed of ASML's position. This date will be no later than two months after the original one month period. An extension of two months may only be sought taking into account the complexity and number of the requests. ASML shall explain the reasons of this delay.

Denial of requests

- 7.4 The rights of Individuals set out in Article 7.1 are subject to any applicable exceptions provided under EEA Data Protection Laws. Depending on the relevant right of the Individual, exceptions may be available in cases where:
- (i) the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of ASML;
 - (ii) the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;
 - (iii) the Processing is necessary for exercising the right of freedom of expression and information;
 - (iv) for dispute resolution purposes;
 - (v) the exercise of the rights by the Individual adversely affects the rights and freedoms of ASML or others; or
 - (vi) in case a specific restriction of the rights of Individuals applies under EEA Law.

The right of access set out in Article 7.1 can only be denied under the

circumstances listed in items (iv), (v), and (vi) above.

ASML may deny a request if:

- (a) the request does not meet the requirements of Article 7.1 or an exception as set out above applies;
- (b) ASML can demonstrate that the request is manifestly unfounded, excessive or not sufficiently specific (and the Individual was given the opportunity to specify his/her request);
- (c) the identity of the relevant Individual cannot be established by reasonable means (and the Individual was given the opportunity to provide additional information necessary to confirm his or her identity); or
- (d) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights.

Notifications of correction or deletion

- 7.5 If ASML grants the Individual's request for rectification or erasure of his or her Personal Data or restriction of the Processing thereof, it shall notify recipients of these Personal Data where reasonably possible and proportional.

Article 8 – Security and Confidentiality Requirements

Data security

- 8.1 ASML shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, take appropriate reasonable technical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, ASML has developed and implemented the ASML Information Security Policies and other policies and guidelines relating to the protection of Personal Data.

Employee access

- 8.2 Staff will be authorized to access Personal Data only as necessary to serve the applicable Processing Purpose and to perform their job as instructed by ASML.

Confidentiality obligations

- 8.3 Staff who access Personal Data will meet their confidentiality obligations.

Data Security Breach notification requirement

- 8.4 Group Companies outside of the EEA shall notify Data Security Breaches without undue delay to ASML Netherlands and relevant Privacy Officers in accordance with ASML's established incident response procedures. Group Companies that act as internal Processors will notify the relevant Group Company that is the Controller of the affected Personal Data without undue delay upon becoming aware of the Data Security Breach. ASML shall notify the Competent Supervisory Authority(s) of a Data Security Breach without undue delay, and where feasible within 72 hours after becoming aware of it, unless the Data Security Breach is unlikely to result in a risk to the rights and freedoms of Individuals. In addition, if the Data Security Breach is likely to result in a high risk to the rights and freedoms of Individuals, ASML shall notify the affected Individuals of the Data Security Breach without undue delay following its determination that such a Data Security Breach has occurred. ASML shall respond promptly to inquiries of Individuals relating to such Data Security Breach. Group Companies shall document Data Security

Breaches (comprising the facts relating to the Data Security Breach, its effects and the remedial action taken) and the documentation should be made available to the Competent Supervisory Authority on request.

Article 9 – Direct Marketing

Direct marketing	9.1	This Article will set forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).
Consent for direct marketing (opt-in)	9.2	If EEA Law so requires, ASML shall only send to Individuals unsolicited commercial electronic communication with the prior consent of the Individual ("opt-in"). If EEA Law does not require prior consent of the Individual, ASML shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.
Exception (opt-out)	9.3	<p>Prior consent of the Individual for sending unsolicited commercial electronic communication will not be required if:</p> <ul style="list-style-type: none">(i) an Individual has provided his electronic contact details to a Group Company in the context of a sale of a product or service of such Group Company;(ii) such contact details are used for direct marketing of such Group Company's own similar products or services; and(iii) provided that an Individual clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his electronic contact details when they are collected by the Group Company.
Information to be provided in each communication	9.4	In every direct marketing communication that is made to the Individual, the Individual will be offered the opportunity to opt-out of further direct marketing communications, including profiling related to this direct marketing.
Objection to direct marketing	9.5	If an Individual objects to receiving marketing communications from ASML, or withdraws his or her consent to receive such materials, ASML will stop sending such further marketing materials, and Processing that Individual's Personal Data for direct marketing purposes, including profiling related to this direct marketing.
Third Parties and Direct marketing	9.6	No Personal Data will be provided to, or used on behalf of, Third Parties for purposes of direct marketing of such Third Party without the prior consent of the Individual.
Direct marketing records	9.7	ASML shall keep a record of Individuals that used their "opt-in" or "opt-out" right and shall regularly check the public opt-out registers.

Article 10 – Automated Decision Making and Profiling

Automated decisions	10.1	Automated tools may be used to make decisions about Individuals, but decisions which produce legal effects concerning him or her or similarly significantly affects the Individual may not be based solely on the results provided by the automated tool. This restriction will not apply if the: <ul style="list-style-type: none"> (i) use of automated tools is necessary for the performance of a task carried out to comply with or authorized by law; (ii) decision is made by ASML for purposes of (a) entering into or performing a contract or (b) managing the contract with the Individual; or (iii) Individual has given his explicit consent.
Special Categories of Data	10.2	ASML will only Process Special Categories of Data for automated decision-making purposes with the Individual's explicit consent or where processing is necessary for reasons of substantial public interest on the basis of EEA Law.
Suitable measures	10.3	In the cases referred to in Article 10.1(ii) and (iii), ASML shall take suitable measures to safeguard the legitimate interests of the Individual, e.g. by providing the Individual with an opportunity to express his or her point of view and at least the right to obtain human intervention on the part of the Controller.

Article 11 – Disclosure and Transfer of Personal Data to Third Parties

Disclosure to Third Parties	11.1	This Article will set forth requirements concerning the disclosure of Personal Data from ASML to a Third Party. Note that a disclosure of Personal Data will include situations in which ASML discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where ASML provides remote access to Personal Data to a Third Party.
Third Party Controllers and Third Party Processors	11.2	There will be two categories of Third Parties: <ul style="list-style-type: none"> (i) Third Party Controllers: these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., ASML Business Partners that provide their own goods or services directly to Business Partners) (ii) Third Party Processors: these are Third Parties that Process Personal Data solely on behalf of ASML and at its direction (e.g., Third Parties that Process online registrations made by Business Partners).
Disclosure for applicable Processing Purposes only	11.3	ASML shall disclose Personal Data to a Third Party to the extent necessary to serve the applicable Processing Purpose for which the Personal Data are Processed (including purposes for which the Individual has provided consent in accordance with Article 2).
Third Party Controller safeguards	11.4	ASML shall seek to contractually safeguard the data protection interests of its Individuals when Personal Data are transferred to Third Party Controllers. This will include the safeguards set forth in Article 11.6
Third Party Processor contracts	11.5	Third Party Processors as well as internal Processors may Process Personal Data only if they have a written contract with ASML. The contract with a Third Party Processor (and/or internal data processor if relevant) will include the following provisions:

- (i) the Third Party Processor shall Process Personal Data only in accordance with ASML's documented instructions and for the purposes authorized by ASML;
- (ii) the Processor shall, and have persons it authorizes to Process Personal Data, keep the Personal Data confidential;
- (iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;
- (iv) the Third Party Processor shall not permit subcontractors and affiliates to Process Personal Data in connection with its obligations to ASML without (a) the prior specific or generic consent of ASML, and (b) a validly entered into written contract between the Third Party Processor and the subcontractor, which imposes data protection obligations that shall be no less protective than those imposed on the Third Party Processor, and provided that the Third Party Processor remains liable to ASML for the performance of the subcontractors. In case ASML gives generic consent, the Third Party Processors shall provide notice to ASML of any changes in its subcontractors and will provide ASML the opportunity to object to such changes based on reasonable grounds;
- (v) the Third Party Processor shall ensure that its subcontractors and affiliates abide by a level of data protection no less protective than the obligations as set out in the contract between the Third Party Processor and ASML;
- (vi) ASML may review the security measures taken by the Third Party Processor and the Third Party Processor shall subject its relevant data processing facilities to audits and inspections by ASML, a Third Party on behalf of ASML or any relevant government authority. This may also be done by means of a statement issued by a qualified independent third party assessor certifying that the information processing facilities of the Third Party Processor used for the Processing of Personal Data comply with the requirements of the contract;
- (vii) the Third Party Processor shall promptly inform ASML of any actual or suspected security breach involving Personal Data;
- (viii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide ASML with all relevant information and assistance as requested by ASML regarding the security breach; and
- (ix) at the choice of ASML, the Third Party Processor shall delete or return all Personal Data to ASML at the end of the provision of services relating to the Processing of Personal Data and shall delete all copies of the Personal Data, unless storing the Personal Data is required by law applicable to the Third Party Processor. The Third Party Processor shall continue to Process the Personal Data in accordance with the requirements of the contract as long as it has not returned or deleted all Personal Data (including copies), and will only retain the Personal Data to the extent and for as long as required under the applicable law.

**Transfer of
Data to a Third
Country**

11.6

This Article sets forth additional rules for the Transfer of Personal Data to a Third Country (including onward transfers). Personal Data may be transferred to a Third Party in a Third Country only:

- (i) in accordance with a data transfer mechanism for the lawful Transfer of Personal Data recognized under EEA Data Protection Law;
- (ii) if (i) does not apply, the Transfer is subject to an applicable derogation for specific situations under EEA Data Protection Law (i.e., the Transfer is necessary for the conclusion or performance of a contract with or in the interest of the Individual (including the implementation of pre-contractual measures taken at the

Individual's request), to protect a vital interest of the Individual, for the establishment, exercise, or defence of a legal claim, or for important reasons of public interest (as recognized by applicable EEA law), or the Individual has given his or her explicit consent to the Transfer, in accordance with Article 11.7).

Item (ii) above requires the prior consultation of the Chief Privacy Officer.

Prior to a Transfer under (i), ASML will conduct a Transfer Impact Assessment in accordance with Article 14.4.

Requirements for consent	11.7	<p>Prior to requesting consent, the Individual will be provided with the following information:</p> <ul style="list-style-type: none"> (i) the purpose of the Transfer; (ii) the identity of the transferring Group Company; (iii) the identity or categories of Third Parties to which the Personal Data will be transferred; (iv) the categories of Personal Data that will be transferred; (v) the country to which the Personal Data will be transferred; and (vi) the fact that the Personal Data will be transferred to a Third Country and the possible risks related to such a Transfer.
---------------------------------	------	--

Article 2.4 will apply to denial or withdrawal of consent.

Consent required by applicable local law for transfer	11.8	<p>If applicable local law so requires, in addition to having one of the grounds listed in Article 11.6, ASML may (also) request (explicit) consent for a Transfer to a Third Party located in a Third Country.</p>
--	------	---

Article 12 – Restrictions under EEA Law

Restrictions under EEA Law	12.1	<p>Certain rights of Individuals and obligations of ASML in these BCR may in specific cases be subject to restrictions provided by EEA law, as specified and applied in accordance with EEA Data Protection Law, such as to:</p> <ul style="list-style-type: none"> (i) prevent or investigate criminal offences (including cooperating with law enforcement); (ii) enforce civil law claims; or (iii) protect Individuals or the rights and freedoms of other persons.
-----------------------------------	------	--

Article 13 – Supervision and Compliance

Chief Privacy Officer	13.1	<p>ASML Holding shall appoint a Chief Privacy Officer who is responsible for:</p> <ul style="list-style-type: none"> (i) establishing a Privacy Board as described in Article 13.2; (ii) supervising compliance with these BCR for Business Partner Data; (iii) coordinating, communicating and consulting with the Privacy Officers on central data protection issues; (iv) providing annual data compliance reports, as appropriate, to the Board of Management or a committee appointed by the Board of Management on data protection risks and compliance issues as described in Article 16.2; (v) maintaining a fully updated list of the Group Companies and keeping records of updates and/or changes to these BCR;
------------------------------	------	---

- (vi) coordinating, in conjunction with the Privacy Officers and the relevant compliance officers, official investigations or inquiries into the Processing of Personal Data by a government authority;
- (vii) dealing with conflicts between these BCR for Business Partner Data and applicable law as described in Article 20;
- (viii) approving Transfers as described in Article 11.6;
- (ix) monitoring the performance and periodic review of a Data Protection Impact Assessment (DPIA) before a new system or a business process involving Processing of Personal Data is implemented;
- (x) monitoring the documentation, notification and communication of Data Security Breaches;
- (xi) deciding on complaints as described in Article 17; and
- (xii) devising the data management processes, systems and tools to implement the framework for data protection management as established by the Privacy Board, including:
 - a) to maintain, update and publish these BCR for Business Partner Data and related policies;
 - b) tools to collect, maintain and update information regarding the structure and functioning of all systems that Process Personal Data;
 - c) data privacy training and awareness for Employees to comply with their responsibilities under these BCR for Business Partner Data;
 - d) appropriate internal audit systems to monitor, audit and report compliance with these BCR for Business Partner Data and ensure that ASML's internal audit department can verify and certify such compliance in line with the ASML periodic assurance process;
 - e) procedures regarding data protection inquiries, concerns and complaints; and
 - f) determine and update appropriate sanctions for violations of these BCR for Business Partner Data (e.g. disciplinary standards).

Privacy Board

- 13.2 The Chief Privacy Officer shall establish a Privacy Board. The Privacy Board shall be made up of the Chief Privacy Officer and Privacy Officers and shall create and maintain a framework for:
- (i) the development, implementation and updating of local Individual data protection statements, policies and procedures;
 - (ii) the maintaining, updating and publishing of these BCR for Business Partner Data and related policies;
 - (iii) the creating, maintaining and updating of information regarding the structure and functioning of all systems that Process Personal Data (as required by Article 14);
 - (iv) the development, implementation and updating of the relevant data protection training and awareness programs;
 - (v) the monitoring, auditing and reporting on compliance with these BCR for Business Partner Data to the Board of Management;
 - (vi) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and
 - (vii) determining and updating appropriate sanctions for violations of these BCR for Business Partner Data (e.g., disciplinary standards).

Privacy Officers

- 13.3 The Chief Privacy Officer shall establish a team of Privacy Officers (also known as Privacy Business Partners within ASML) sufficient to direct compliance with these BCR for Business Partner Data within ASML.

The Privacy Officers will perform the following tasks:

- (i) implement the data management processes, systems and tools, devised by the Chief Privacy Officer to implement the framework

- for data protection management established by the Privacy Board within ASML;
- (ii) support and assess overall data protection management compliance within ASML;
 - (iii) regularly advise the business and the Chief Privacy Officer on privacy risks and compliance issues;
 - (iv) maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that Process Personal Data (as required by Article 14.2);
 - (v) be available for requests for privacy approvals or advice as described in Article 7;
 - (vi) provide information relevant to the annual privacy report of the Chief Privacy Officer (as required in Article 16);
 - (vii) assist the Chief Privacy Officer in the event of official investigations or inquiries by government authorities;
 - (viii) own and authorize all appropriate privacy processes and procedures within ASML;
 - (ix) advise the business with regard to the deletion, destruction, anonymization or transfer of stored data as required by Article 5.2;
 - (x) decide on and notify the Chief Privacy Officer of complaints as described in Article 17; and
 - (xi) cooperate with the Chief Privacy Officer, other Privacy Officers, and the general business principles compliance officers to:
 - ensure that the instructions, tools and training are in place to enable ASML to comply with these BCR for Business Partner Data;
 - share and provide guidance on best practices for data protection management within ASML;
 - ensure that data protection requirements are taken into account whenever new technology is implemented within ASML; and
 - notify the business of the involvement of external service providers with data processing tasks.

Privacy Officers will be responsible for:

- (xii) consulting with the Chief Privacy Officer in all cases where there is a conflict between applicable law and these BCR for Business Partner Data as described in Article 20; and
- (xiii) informing the Chief Privacy Officer of any new legal requirement that may interfere with ASML's ability to comply with these BCR for Business Partner Data as required by Article 20.

Privacy Champion

13.4 The Chief Privacy Officer shall appoint Privacy Champions within different ASML departments. The Privacy Champions will be ASML employees that promote privacy awareness within their department and are responsible for:

- (i) supporting and facilitating compliance with the EEA Data Protection Laws within their respective organizations;
- (ii) raising questions and issues with the Chief Privacy Officer and the Privacy Officers; and
- (iii) identifying cases where privacy may be a topic of interest within a process, asset or way of working and ensuring that the correct action is taken.

Article 14 – Policies and Procedures

Policies and procedures	14.1	ASML shall develop and implement policies and procedures to comply with these BCR for Business Partner Data.
Records of Processing Activities	14.2	ASML will maintain Records of Processing Activities. A copy will be provided to the Competent Supervisory Authority upon request.
Data Protection Impact Assessment (DPIA)	14.3	<p>ASML shall conduct a Data Protection Impact Assessment (DPIA) for the Processing operations that are likely to result in a high risk to the rights and freedoms of individuals. The DPIA will be performed prior to implementation of the envisaged IT system or Processing.</p> <p>The outcome of a DPIA is to identify the necessary measures to minimize risk and comply with applicable data protection law and the GDPR. The DPIA will amongst other things take into account the risks to the privacy rights of Individuals including a description of mitigating (privacy-by-design and privacy-by-default) measures to minimize these risks. Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by ASML, the Processing of Personal Data still presents a residual high risk for the rights and freedoms of Individuals, the Competent Supervisory Authority will be consulted prior to Processing taking place.</p>
Transfer Impact Assessment	14.4	<p>ASML will perform a Transfer Impact Assessment prior to the Transfer of Personal Data under these BCR and maintain it for the duration of the Transfer.</p> <p>Where a Transfer Impact Assessment shows gap(s) in protection for Individuals under these BCR, ASML will implement supplementary measures, such as contractual, technical, or organizational safeguards, including measures applied during transmission and to the Processing of Personal Data in the country of destination to ensure compliance with these BCR. Supplementary measures are not required in relation to laws and practices applicable to the Data Importer that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR.</p> <p>The Transfer shall not take place or will be suspended where: (i) compliance with these BCR cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent Supervisory Authority.</p> <p>ASML will conduct and document the Transfer Impact Assessment with the involvement of ASML Netherlands and the Chief Privacy Officer and will notify the Data Exporter and Data Importer thereof. ASML Netherlands and the Chief Privacy Officer will make the Transfer Impact Assessment, including any applicable supplementary measures, available to all Group Companies, so that the same supplementary measures are applied to the same types of Transfers, and to any Competent Supervisory Authority upon request.</p>
Privacy-by-design and privacy-by-default	14.5	ASML considers data protection an integral component of the design, development, operation and management of new projects and processes which involve Personal Data. To this end, ASML shall take reasonable efforts to integrate privacy into the developing and designing process of the aforementioned projects and processes, including projects and processes where ASML engages third parties as part of any design, development and

implementation work.

Article 15 – Training

- | | | |
|-----------------------|------|--|
| Staff training | 15.1 | ASML shall provide bi-annual training on the obligations and principles laid down in these BCR for Business Partner Data and related confidentiality obligations to Staff who have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to Process Personal Data. |
|-----------------------|------|--|

Article 16 – Monitoring and Auditing Compliance

- | | | |
|---|------|---|
| Audits | 16.1 | <p>ASML Internal Audit and external auditors (if any) shall audit business processes and procedures that involve the Processing of Personal Data for compliance with all aspects of these BCR for Business Partner Data, including methods of ensuring that corrective actions will take place. Privacy is a recurring topic part of ASML's bi-annual audit activities. The audits may be carried out in the course of the regular activities of ASML Internal Audit or initiated by the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. ASML Internal Audit may include privacy aspects in every individual audit even if the main subject of the audit does not relate to privacy (meaning that an audit into HR may also include a check of privacy aspects, e.g. access rights to Employee Data within the HR department). All corrective action plans resulting from the audit will be followed up and reported upon by Internal Audit.</p> <p>Applicable professional standards of independence, integrity and confidentiality will be observed when conducting an audit. The Chief Privacy Officer, ASML Holding, ASML Netherlands and the appropriate Privacy Officers will be informed of the results of the audits. ASML shall provide a copy of the audit results to the Competent Supervisory Authority upon its request.</p> |
| Annual Privacy Report | 16.2 | <p>The Chief Privacy Officer shall produce an annual data compliance report for the Board of Management or a committee appointed by the Board of Management on compliance with these BCR for Business Partner, data protection risks and other relevant issues.</p> <p>Each Privacy Officer shall provide information relevant to the report to the Chief Privacy Officer.</p> |
| Mitigation | 16.3 | ASML shall, if so indicated, ensure that adequate steps are taken to address breaches of these BCR for Business Partner Data identified during the monitoring or auditing of compliance pursuant to this Article 16. |
| Audit or inspection by Supervisory Authority | 16.4 | The Competent Supervisory Authority may request an audit or to carry out an inspection (including where necessary on-site) of the facilities used by ASML for the Processing of Personal Data for compliance with these BCR. ASML shall cooperate with the Competent Supervisory Authority in respect of such audit or inspection. |

**Advice of the
Supervisory
Authorities**

- 16.5 ASML shall: (a) provide to the Competent Supervisory Authorities, upon request, information in relation to the Processing of Personal Data which is subject to these BCR; and (b) take into account the advice of, and abide by binding decisions of, the Competent Supervisory Authorities issued on the interpretation and application of these BCR.

Article 17 – Complaints Procedure

Complaint

- 17.1 Individuals may file a complaint regarding compliance with these BCR for Business Partner Data or violations of their rights under these BCR in accordance with the complaints procedure set forth in the relevant privacy policy or contract, or by emailing privacyoffice@asml.com (or using the contact details set out in Article 22.4 below). The complaint will be forwarded to the appropriate Privacy Officer.

The appropriate Privacy Officer shall:

- (a) notify the Chief Privacy Officer and applicable legal counsel;
- (b) initiate an investigation together with the applicable legal counsel; and
- (c) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

The appropriate Privacy Officer or applicable legal counsel may, upon prior approval of the Chief Privacy Officer, consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

**Reply to
Individual**

- 17.2 Without prejudice to Article 7 of these BCR for Business Partner Data (Individual rights), the appropriate Privacy Officer shall inform the Individual without undue delay and in any event within one month of ASML receiving a complaint in writing or electronically either (a) of ASML's position with regard to the complaint and any action ASML has taken or will take in response or (b) when he will be informed of ASML's position, which date will be no later than two months thereafter, taking into account the complexity and number of requests. The appropriate Privacy Officer shall send a copy of the complaint and his or her written reply to the Chief Privacy Officer.

**Complaint to
Chief Privacy
Officer**

- 17.3 An Individual may file a complaint with the Chief Privacy Officer if:
- (i) the resolution of the complaint by the appropriate Privacy Officer is unsatisfactory to the Individual (e.g., the complaint is rejected)
 - (ii) the Individual has not received a response as required by Article 17.2
 - (iii) the time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response or
 - (iv) in one of the events listed in Article 7.4.

The procedure described in Articles 17.1 through 17.2 will apply to complaints filed with the Chief Privacy Officer. An Individual may at all times file a complaint or claim with the Supervisory Authority or the competent court in accordance with Article 18.4, including if the handling of the complaint by the Chief Privacy Officer is not satisfactory to the Individual.

Article 18 – Legal Issues

Interaction with Local Law	18.1	Individuals may enforce the commitments made by ASML under these BCR in accordance with this Article 18. These rights are in addition to, and will not prejudice, any other rights or remedies that these Individuals may otherwise have against ASML under applicable law.
Competent Court for Disputes Related to SA Supervision	18.2	Any dispute related to the Competent SA's exercise of supervision of compliance with these BCR will be resolved by the courts of the Member State of that SA, in accordance with that Member State's procedural law. The Group Companies agree to submit themselves to the jurisdiction of these courts.
Out of court settlement option	18.3	Individuals are encouraged (but are not required) to first file a complaint with ASML in accordance with Article 17 before filing a complaint or claim with a Supervisory Authority or court in accordance with Article 18.4.
Jurisdiction for Claims of Individuals	18.4	<p>In case of a violation of these BCR, the affected Individual may, at his or her choice, submit a complaint or a claim (as applicable) under Article 18.6 to:</p> <ul style="list-style-type: none">(i) The courts in the EEA country (a) where the Individual has his or her habitual residence, or (b) where the Group Company being the Controller or the internal Processor of the relevant Personal Data is established, against the Group Company being the Controller or the internal Processor of the relevant Personal Data or ASML Netherlands;(ii) The SA in the EEA country where (a) the Individual has his or her habitual residence or place of work, or (b) the alleged infringement took place, against the Group Company being the Controller or the internal Processor of the relevant Personal Data or ASML Netherlands; or(iii) The Lead SA or the courts in the Netherlands, against ASML Netherlands. <p>ASML Netherlands accepts liability for a breach by a Group Company located outside the EEA, although ASML Netherlands may assert any defense that the relevant non-EEA Group Company could have asserted.</p> <p>Individuals may be represented by a not-for-profit body, organization, or association under the conditions set out in EEA Data Protection Laws.</p>
Damages and available remedies, burden of proof	18.5	<p>In case an Individual has a claim under Article 18.6, such Individual shall be entitled to compensation of material and non-material damages suffered by such Individual resulting from a violation of these BCR to the extent provided by applicable law of the relevant EEA country.</p> <p>To bring a claim for damages, the Individual must demonstrate that he or she has suffered damages and establish facts which show it is likely that the damage has occurred because of a violation of these BCR. If ASML Netherlands can prove that the Group Company or Third Party Processor located outside the EEA is not responsible for the event giving rise to the damage, it may discharge itself from liability.</p>
Third party beneficiary	18.6	Without prejudice to anything in these BCR for Business Partner Data, Individuals may enforce the following elements of these BCR for Business

rights

Partner Data as third-party beneficiaries:

- (i) Data protection principles (Articles 2, 3, 4, 5, 6, 8 and 11);
- (ii) Transparency and easy access to these BCR for Business Partner Data (Articles 1.5 and 6);
- (iii) Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated Processing, including profiling (Articles 7 and 10);
- (iv) Obligations in case of local laws and practices affecting compliance with these BCR for Business Partner Data and in case of Disclosure Requests (Article 20 and 14.4);
- (v) Privacy by design and default (Article 14.5);
- (vi) Right to complain through the internal complaint mechanism of the companies (Article 17);
- (vii) Cooperation duties with Supervisory Authorities (Article 16.4 and 16.5);
- (viii) Liability and jurisdiction provisions (Article 18);
- (ix) Duty to inform of updates to these BCRs and the Group Companies (Article 21.3).

Mutual assistance and redress

18.7 All Group Companies will co-operate with and assist each other to the extent reasonably possible to handle:

- (i) a request, complaint or claim made by an Individual; or
- (ii) a lawful investigation or inquiry by a competent Supervisory Authority or competent government authority.

The Group Company who receives a request, complaint or claim from an Individual will be responsible for handling any communication with the Individual regarding his or her request, complaint or claim except where circumstances dictate otherwise.

ASML Netherlands shall take the necessary actions to address violations of these BCR by Group Companies in Third Countries and to pay compensation for any material or non-material damage resulting from such a violation in accordance with Article 18.5. The Group Company in a Third Country that is responsible for the Processing to which a request, complaint or claim relates, will bear all costs involved and reimburse ASML Netherlands.

Article 19 – Sanctions for Non-compliance**Non-compliance**

19.1 Non-compliance of Employees with these BCR for Business Partner Data may result in appropriate measures in accordance with applicable local law up to and including termination of employment.

Article 20 – Conflicts between these BCR for Business Partner Data and Applicable Local Law and Termination of Transfers**Notification of Conflicts**

20.1 Each Data Importer shall monitor its local laws and practices. If a Data Importer becomes aware that it is unable to comply with these BCR, including if it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with these BCR or that have a substantial effect on the protection offered by these BCR (including

on any Data Protection Impact Assessments or Transfer Impact Assessments performed thereunder), the relevant Data Importer will promptly notify the relevant Data Exporter and ASML Netherlands.

The relevant Data Exporter and ASML Netherlands shall, following a verification of such notification, determine, in consultation with the relevant Data Importer and the Chief Privacy Officer, how to comply with these BCR and address a potential conflict, including by implementing appropriate supplementary measures in accordance with Article 14.4.

Laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of the GDPR, are not considered to prevent ASML from complying with these BCR or to have a substantial effect on the protection offered by these BCR.

The Data Exporter will monitor on an ongoing basis, and where appropriate in collaboration with the Data Importer, developments in the Third Country that could affect the initial Transfer Impact Assessment performed under Article 14.4.

**Consequences
of Termination
of a Transfer**

20.2 The Data Importer shall – at the Data Exporter’s option – immediately return or delete Personal Data that were received under these BCR (including any copies thereof), and certify to the Data Exporter that it has done so, where: (i) the Transfer has been suspended in accordance with Article 14.4 for a period longer than one month, (ii) the Data Importer is in substantial or persistent breach of these BCR, (iii) the Data Importer fails to comply with a binding decision of a Competent SA or court, or (iv) the Data Importer ceases to be bound by these BCR. If local laws applicable to the Data Importer prevent the return or deletion of Personal Data, the Data Importer will only process the Personal Data to the extent and for as long as required under that local law. Until the Personal Data are deleted or returned, the Data Importer will continue to ensure a level of protection no less than that provided for in these BCR.

**Disclosure
Requests**

20.3 Subject to the following paragraph, the Data Importer shall inform the Individual (where possible and with the help of the Data Exporter) and the Data Exporter, if the Data Importer receives a Disclosure Request. Notifications of a Disclosure Request shall include information about the Personal Data requested, the requesting body, the legal basis for the request and the provided response. In case of direct access to Personal Data by a public authority in the Destination Country, the notification will include all information available to the Data Importer.

The Data Importer will assess the legality of a Disclosure Request, in particular whether it remains within the powers granted to the requesting authority. The Data Importer will challenge Disclosure Requests that it considers unlawful under the laws of the Destination Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, the Data Importer shall seek interim measures with a view to suspending the effects of the Disclosure Request until the competent judicial authority has decided on its merits. The Data Importer shall not disclose the Personal Data requested until required to do so under the applicable procedural rules and will only provide the Personal Data that are strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. The Data Importer will document this assessment and provide it to the Data Exporter and, upon request, to any Competent SA.

If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, the Data Importer will inform the Data Exporter to the maximum extent permitted by applicable law, and will use its best efforts to waive this prohibition, will document these efforts, and demonstrate them upon request to the Data Exporter. The Data Importer will at regular intervals provide the Data Exporter with as much relevant information as possible on the requests received (such as the number of requests, type of Personal Data requested, requesting authority, whether requests have been challenged and the outcome of such challenges). This information will be preserved and provided to any Competent SA upon request. If the Data Importer is or becomes partially or completely prohibited from providing such information to the Data Exporter, it will (without undue delay) inform the Data Exporter of such a prohibition.

The Data Importer will provide the minimum amount of information permissible when responding to a Disclosure Request. In any event, any disclosures by the Data Importer of Personal Data to any authority in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Article 21 – Changes to these BCR for Business Partner Data

Approval for Changes	21.1	Any changes to these BCR for Business Partner Data will require the prior approval of the Chief Privacy Officer. All Group Companies will be informed of changes to these BCR for Business Partner Data as per the Article 1.5. The Chief Privacy Officer shall keep a record of any changes made to these BCR for Business Partner Data and will notify any changes including any updates to the list of Group Companies, to the relevant SAs via the Lead SA on a yearly basis, including a brief explanation of the reasons justifying the update. Where a change affects the protection offered by these BCR for Business Partner Data or significantly affects these BCR for Business Partner Data itself (e.g., changes to the binding character), the Chief Privacy Officer will promptly communicate these to the relevant SAs via the Lead SA in advance.
	21.2	These BCR for Business Partner Data may be changed by ASML Netherlands without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.
Effective Date of Changes	21.3	Any change will enter into force with immediate effect after it has been approved in accordance with Article 21.1 and is published on the ASML website and its intranet.
		The published version of these BCRs will include Article 1 and the Articles listed in Article 18.6, including the Annexes 1 – 3 to these BCR.
Prior Versions	21.4	Any request, complaint or claim of an Individual relating to any Group Company involving these BCR for Business Partner Data will be evaluated against the version of these BCR for Business Partner Data that is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

General transition period	22.1	Except as indicated below, Group Companies shall comply with these BCR for Business Partner Data as soon as reasonably possible and in any case within two years of the Effective Date.
No transfer during transition period	22.2	No Transfer based on these BCR for Business Partner Data will be made unless a Group Company complies with these BCR, including during the transition periods. Until such time that a Group Company can demonstrate compliance with these BCR, the Transfer will be made based on another legal basis for Transfer under EEA Data Protection Law, such as standard contractual clauses.
Transition Period for Divested Entities	22.3	A Divested Entity may remain a Group Company for purposes of these BCR for Business Partner Data after its divestment for such period as may be required by ASML to disentangle the Processing of Personal Data relating to such Divested Entity. If a Data Importer in a Third Country ceases to be an ASML Group Company or bound by these BCR, it may keep the Personal Data received under these BCR (i) if it continues to comply with these BCR, or (ii) on the basis of another legal basis for data Transfer under EEA Data Protection Law, such as standard contractual clauses.
Contact details	22.4	ASML Privacy Office c/o ASML Netherlands B.V. De Run 6501, 5504 DR Veldhoven, the Netherlands E-mail: privacyoffice@asml.com
Company structure	22.5	https://www.asml.com/contacts/main-offices/en/s223?rid=7657 .

ANNEX 1**Definitions**

Adequacy Decision	ADEQUACY DECISION means a decision issued by the European Commission under Article 45(3) of the GDPR that a country or region outside the EEA or a category of recipients in such country or region is deemed to provide an “adequate” level of data protection.
ASML	ASML means ASML Holding and its Group Companies.
ASML Holding	ASML HOLDING means ASML Holding N. V., having its registered seat in Veldhoven, the Netherlands
ASML Netherlands	ASML NETHERLANDS means ASML Netherlands B.V., having its registered seat in Veldhoven, the Netherlands.
BCR or BCR for Business Partner Data	BCR or BCR FOR BUSINESS PARTNER DATA means these ASML Binding Corporate Rules for Business Partner Data and any amendments thereto.
Board of Management	BOARD OF MANAGEMENT means the board of directors of ASML Holding.
Business Partner	BUSINESS PARTNER means a Customer, Supplier or any Third Party, that has or had a business relationship or strategic alliance with ASML (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE means a purpose for Processing Personal Data as specified in Annex 3 and Article 2 or 3 or for Processing Special Categories of Data as specified in Annex 3 and Article 4 or 3.
Chief Privacy Officer	CHIEF PRIVACY OFFICER means the officer as referred to in Article 13.1.
Code of Conduct	CODE OF CONDUCT means the ASML Code of Conduct available here and as updated from time to time.
Competent SA or Competent Supervisory Authority	COMPETENT SA or COMPETENT SUPERVISORY AUTHORITY means the Supervisory Authority competent for the Data Exporter(s) of the specific Transfer.
Controller	CONTROLLER means 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 EEA law, the Controller or the specific criteria for its nomination may be provided for by EEA law.
Criminal Data	CRIMINAL DATA means Personal Data relating to criminal convictions and offences or related security measures, including Personal Data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior.
Customer	CUSTOMER means any organization that purchases, may purchase or has purchased an ASML product or service.
Customer Services	CUSTOMER SERVICES means the services provided by ASML to Customers to support ASML products offered to or in use with Customer employees. These services may include the maintenance, upgrade, inspection and related support activities aimed at facilitating continued and sustained use of ASML products (e.g. servicing equipment).
Data Exporter	DATA EXPORTER means the Group Company that Transfers Personal Data to a Third Country under these BCR.
Data Importer	DATA IMPORTER means the Group Company in a Third Country that is the

recipient of a Transfer of Personal Data under these BCR.

**Data Protection
Impact Assessment
(DPIA)**

DATA PROTECTION IMPACT ASSESSMENT (DPIA) means a review procedure to carry out and document an assessment of the impact of an envisaged IT-system or Processing on the protection of Personal Data and Individuals' privacy rights. The DPIA will be performed prior to implementation of the envisaged IT-system or Processing and will regard the entire lifecycle management of Personal Data, from collection to Processing to deletion. A DPIA contains a description of:

- the relevant ASML Group Companies and third parties responsible for the Processing;
- the envisaged Processing;
- the Business Purpose for which Personal Data are Processed;
- security measures;
- data retention periods;
- categories of recipients; and
- any Transfers to a Third Country, including suitable transfer mechanisms;

and an assessment of:

- the necessity and proportionality of the envisaged Processing;
- the risks to the privacy rights of Individuals including a description of mitigating (privacy-by-design and privacy-by-default) measures to minimize these risks; and
- the context of the Processing.

Data Security Breach

DATA SECURITY BREACH means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of, or access to, Personal Data transmitted, stored or otherwise Processed.

Destination Country

DESTINATION COUNTRY means the Third Country to which Personal Data are transferred.

Disclosure Request

DISCLOSURE REQUEST means a legally binding request for disclosure of (or direct access to) Personal Data from a public authority of a Destination Country.

Divested Entity

DIVESTED ENTITY means the divestment by ASML of a Group Company or business by means of:

- (a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company; and/or
- (b) a demerger, sale of assets, or any other manner or form.

**Dutch Supervisory
Authority or Lead SA**

DUTCH SUPERVISORY AUTHORITY or LEAD SA means the Dutch supervisory authority (*Autoriteit Persoonsgegevens*).

**EEA or European
Economic Area**

EEA or EUROPEAN ECONOMIC AREA means all Member States of the European Union, plus Norway, Iceland and Liechtenstein.

EEA Law

EEA LAW means the laws and regulations of the EEA applicable to ASML as the case may be from time to time.

**EEA Data Protection
Law**

EEA DATA PROTECTION LAW means the provisions of mandatory law of an EEA country containing rules for the protection of Individuals with regard to the Processing of Personal Data including security requirements for and the free movement of such Personal Data.

Effective Date	EFFECTIVE DATE means the date on which these BCR for Business Partner Data become effective as set forth in Article 1.5.
Employee	<p>EMPLOYEE means the following persons:</p> <ul style="list-style-type: none"> (a) an employee, job applicant or former employee of ASML including temporary workers working under the direct supervision of ASML (e.g. independent contractors and trainees). This term does not include people working at ASML as consultants or employees of Third Parties providing services to ASML; and (b) a (former) executive or non-executive director of ASML or (former) member of the supervisory board or similar body to ASML.
General Data Protection Regulation ("GDPR")	GENERAL DATA PROTECTION REGULATION means 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 any EU member state implementation act as mandated by the GDPR.
Group Company	GROUP COMPANY means ASML Holding and any company or legal entity of which ASML Holding, directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as it is covered by the ASML Code of Conduct .
Individual	INDIVIDUAL means any (employee of or any person working for) a Business Partner and any other individual who's Personal Data ASML processes in the context of the manufacturing of its products and the sale of these products and the provision of related services.
Internal Audit	INTERNAL AUDIT means the internal audit department of a Group Company or ASML Netherlands.
Original Purpose	ORIGINAL PURPOSE means the purpose for which Personal Data was originally collected.
Personal Data or Data	PERSONAL DATA OR DATA means any information relating to an identified or identifiable Individual.
Privacy Board	PRIVACY BOARD means the board referred to in Article 13.2.
Privacy Champion	PRIVACY CHAMPION means the privacy champion referred to in Article 13.4.
Privacy Officer	PRIVACY OFFICER means a privacy officer (also known as a Privacy Business Partner within ASML) appointed by the Chief Privacy Officer pursuant to Article 13.3.
Processing	PROCESSING means any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
Processor	PROCESSOR means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
Records of	RECORDS OF PROCESSING ACTIVITIES means a record of Processing activities maintained in writing, including in electronic form, by ASML that

Processing Activities	<p>contains the following information:</p> <ol style="list-style-type: none"> the name and contact details of the ASML Group Company that is the Controller; the Processing Purposes; the categories of Personal Data and the categories of data subjects; the categories of recipients to whom Personal Data have been disclosed; where applicable, information about Transfers to a Third Country; where possible, the envisaged retention periods; and where possible, a general description of the measures under Article 8.1. <p>Where an ASML Group Company acts as an internal Processor, the Records of Processing Activities shall:</p> <ol style="list-style-type: none"> in addition include the name and contact details of the ASML Group Company that is the Processor, and instead of b – d above, include the categories of Processing carried out on behalf of the ASML Group Company that is the Controller.
Secondary Purpose	SECONDARY PURPOSE means any purpose other than the Original Purpose for which Personal Data is further Processed.
Special Categories of Data	SPECIAL CATEGORIES OF DATA means Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, social security numbers issued by the government, or genetic and biometric data for the purpose of uniquely identifying a natural person.
Staff	STAFF means all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using ASML information technology systems or working primarily from ASML's premises.
Supervisory Authority or SA	SUPERVISORY AUTHORITY or SA means an EEA supervisory authority, duly constituted and competent in accordance with the applicable EEA Data Protection Law.
Supplier	SUPPLIER means any Third Party that provides goods or services to ASML (e.g. an agent, consultant or vendor).
Third Country	THIRD COUNTRY means a country outside the EEA to which Personal Data are transferred, where such Transfer is not covered by an Adequacy Decision.
Third Party	THIRD PARTY means any person, private organization or government body outside ASML.
Third Party Controller	THIRD PARTY CONTROLLER means a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Personal Data on behalf of ASML that is not under the direct authority of ASML.
Transfer	TRANSFER means a transfer (or set of transfers) of, including disclosure of, or remote access to, Personal Data that are subject to EEA Data Protection Law to a Third Country.
Transfer Impact Assessment	TRANSFER IMPACT ASSESSMENT means an assessment on whether, taking into account the specific circumstances of the Transfer, the laws and practices of the Destination Country, including those requiring the disclosure of

Personal Data to public authorities or authorizing access by such authorities, prevent ASML from fulfilling its obligations under these BCR. Laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in article 23(1) GDPR, are understood not to be in contradiction with these BCR.

In assessing the laws and practices of the Destination Country, ASML shall take into account in particular:

(i) the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Destination Country or to another Destination country, including:

- purposes for which data are transferred and Processed (e.g., marketing, HR, storage, IT support);
- types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
- sector in which the Transfers occur;
- categories and format of the Personal Data transferred;
- location of the Processing including storage;
- transmission channels used.

(ii) the laws and practices of the Destination Country relevant in light of the circumstances of the Transfers, including requirements to disclose Personal Data to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Personal Data during transit between the country of the Data Exporter and the Destination Country;

(iii) any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under these BCR, including measures applied during transmission and to the Processing of Personal Data in the Destination Country.

Interpretations

INTERPRETATION OF THESE BCR FOR BUSINESS PARTNER DATA:

- (i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;
- (ii) headings are included for convenience only and are not to be used in construing any provision of these BCR for Business Partner Data;
- (iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- (iv) the male form shall include the female form;
- (v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;
- (vi) a reference to a document (including, without limitation, a reference to these BCR for Business Partner Data) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these BCR for Business Partner Data or that other document; and
- (vii) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2 – List of Group Companies covered by these BCR for Business Partner Data

The below list covers ASML Holding and the Group Companies that are bound by these BCR as per October 2026. The inclusion or omission of an entity from the list below shall not be determinative of whether such entity is a Group Company. Any entity that satisfies the definition of Group Company shall be deemed covered by and bound by these BCR:

Legal entity	Jurisdiction of incorporation
ASML (Beijing) Equipment Repair Company Limited	China
ASML (Shanghai) Electrical Equipment Co. Ltd.	China
ASML (Shanghai) Lithography Facilities Science and Technology Co., Ltd.	China
ASML (UK) Limited	UK
ASML Belgium BV	Belgium
ASML Berlin AG	Germany
ASML Equipment Malaysia Sdn. Bhd.	Malaysia
ASML France SARL	France
ASML Germany GmbH	Germany
ASML Holding N.V.	Netherlands
ASML Hong Kong Limited	Hong Kong SAR
ASML India Private Limited	India
ASML Ireland Limited	Ireland
ASML Israel (2001) Ltd.	Israel
ASML Italy S.r.l.	Italy

Legal entity	Jurisdiction of incorporation
ASML Japan Co. Ltd.	Japan
ASML Korea Co., Ltd.	South Korea
ASML Netherlands B.V.	Netherlands
ASML Participations Germany GmbH	Germany
ASML Repair Center Korea Ltd.	South Korea
ASML Singapore Pte. Ltd.	Singapore
ASML Taiwan Limited	Taiwan
ASML Technology Taiwan Limited	Taiwan
ASML Trading B.V.	Netherlands
ASML US, LP	US
ASML US, LLC	US
Brion Technologies (Shenzhen) Co. Ltd.	China
Cymer B.V.	Netherlands
Cymer Japan, Inc.	Japan
Cymer Korea Inc.	South Korea
Cymer Semiconductor Equipment (Shanghai) Co., Ltd.	China
Cymer Singapore Pte. Ltd.	Singapore
Cymer Southeast Asia Limited	China

Legal entity	Jurisdiction of incorporation
Cymer, LLC	US
Hermes Microvision Incorporated B.V.	Netherlands

ANNEX 3 – Description of Processing of Business Partner Data

This table sets out the types of Individuals we may Process Personal Data about, the categories of Personal Data we may Process about them, and the purposes for which we Process Personal Data. This table is intended to be a generic summary rather than an exhaustive list. It does NOT mean we Process this data about all these types of Individuals.

Categories of Individuals	<ul style="list-style-type: none"> • Customers include customer contacts, current and past contacts and prospects. • Business Partners include contact persons of organizations that have a business relationship or strategic alliance with ASML (e.g. joint marketing partner, joint venture or joint development partner). • Suppliers include contact persons of vendors, suppliers, advisors, agents, consultants and other professional experts. • Stakeholders include government officials, members of the press and other organizations that collaborate, communicate, or otherwise interact with ASML (including charities, educational institutions, regulators, business intermediaries). • Users include website users and complainants, correspondents and enquirers. • Attendees include individuals attending our events or actions. • Other Individuals include other third parties.
Categories of Personal Data	<p>Personal Data categories</p> <ul style="list-style-type: none"> • Personal details (customers & prospects): e.g. name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, data relating to goods and services provided or obtained, relationship with ASML, data related to events and visits (invitations, attendance, relevant costs).

- **Personal details (vendors, service providers, suppliers, payees and intermediaries, legal services data):** e.g. name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address); preferred language for communications; data related to invitations for business trips or other business events (e.g., itinerary, costs); entity tax identification number and commercial registry registration number; entity bank details and payment related information, bill to addresses, billing currency; VAT (or equivalent) number; vendor/supplier number or other unique identifier; country registration number; information derived from the deployment and use of information systems and tools including from third parties; curriculum vitae; time and expense records concerning the provision of services; operational data; details of relationship with ASML.
- **Interaction data:** e.g. correspondence with ASML, newsletter preferences, technical details to enable website use (e.g. IP address), details on website use, contact preferences, preferred language for communications, marketing preferences, data relating to interaction or relationship with ASML - enquiry, complaint, site visit, application for award, grant, educational initiative.
- **Website, tools, systems, apps:** e.g. information required to access ASML systems, tools and applications, e-mail account, instant messaging account, system passwords, access logs, access rights, security level, activity logs, country code, company details, department details, electronic content produced using ASML systems, information derived from the deployment and use of information systems and tools including from third parties; IP addresses, individual posts into internal communities, comments, systems' recordings such as web meetings, calls and webinars.
- **Advertising, marketing and public relations:** e.g. advertising, marketing and PR related activities; communications; research, complaints and enquiries handling; management of business relationships and other activities.
- **Accounts and records data, data relating to customers, vendors, service providers, suppliers, payees and intermediaries, legal services data:** e.g. customer ID; title; employer, department; location, billing, credit analysis, account maintenance, internal administration and accounting for all commercial relationships; managing and analyzing sales and demand; communications; business operations; customer relationship management; conducting internal audits and other internal control activities relating to contract; management with customers, suppliers, vendors, subcontractors and business partners; compliance; due diligence for anticorruption and anti-bribery purposes; reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments, internal investigations; legal filing and reporting; purchase order and payment; other services on an ad-hoc basis.
- **Data relating to mergers, ventures and acquisitions:** e.g. management and employment information, compensation and payroll data, business operations, customer relationship management, compliance; due diligence, reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments; legal filing and reporting.

Special Categories of Data categories:

- See the categories of Special Categories of Data set forth in article 4 BCR for Business Partner Data.

Purposes for which ASML uses Personal Data	The purposes for which ASML Processes Personal Data can be found in articles 2 (Personal Data) and 4 (Special Categories of Data) of these BCR for Business Partner Data. Examples of Processing Activities are also provided immediately below:		
	Category of Group Companies	Purpose of Processing	Examples of Processing Activities
	All Group Companies	Business communication	Communicating with (prospective) customers, such as, answering questions or replying to communications.
	All Group Companies	Customer assessment and acceptance	Customer assessment and acceptance processes, such as, confirming and verifying identity, due diligence, and screening against publicly available government and/or law enforcement agency sanctions lists.
	All Group Companies	Concluding and executing agreements	Administrative processes, such as, sending invoices, making payments, delivering or receiving services, including related customer services.
	All Group Companies	Monitoring and investigating compliance	Monitoring and/or investigating compliance with EEA Laws, regulations, and/or ASML policy or conditions, anti-money laundering and anti-terrorism screening.
	All Group Companies	Website and/or mobile app usage	Providing functionalities of websites and mobile apps, including administering user accounts, improving performance, saving preferences or products, enabling sharing functionalities.
	All Group Companies	Compliance with law	Complying with obligations under EEA Laws and regulations, such as, tax or business conduct related obligations.
	All Group Companies	Protecting health, safety, security and ensuring integrity	Safeguarding the health and safety of ASML employees, customers, suppliers and business partners, such as, via

			access controls to ASML's systems and premises, sanctions checks against publicly available sanctions lists, protecting premises using CCTV cameras, using road-facing cameras on trucks transporting hazardous materials, and using telemetry on tanks used to store hazardous materials to ensure proper maintenance.
	All Group Companies	Business process execution and internal management	General management, order management and asset management, such as, leveraging central processing facilities in order to work more efficiently, conducting audits and investigations, implementing business controls, managing and using customer, supplier and business partner directories, finance, accounting, archiving, insurance, legal and business consulting, and dispute resolution.
Recipients	<ul style="list-style-type: none"> • ASML Group Companies, includes ASML Group Companies which are regulated by these BCR. • Professional advisors, includes accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors. • Service providers, companies that provide products and services to ASML such as payroll, pension scheme, benefits providers, human resources services, performance, training, expense management, IT systems suppliers and support, third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers. • Public and governmental authorities, includes bodies that regulate or have jurisdiction over ASML such as regulatory authorities, law enforcement, public bodies, and judicial bodies. • Corporate / commercial transaction, includes third parties in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of ASML business, assets or stock (including in connection with any bankruptcy or similar proceedings). A third party in connection with any proposed or actual customer project. 		

Countries to which Transfers may be made	Many of our global systems are operated from the European Union, we also have significant operations in North America and Asia. However, as a global group of companies, ASML continuously transfers Personal Data between its various Group Companies. As such, Personal Data may be transferred between the various Group Companies for the purposes, and in relation to the categories of Personal Data, included in this Annex 3. A list of ASML Group Companies between which Personal Data may be transferred is available as Annex 2 to these BCR.
---	---