JPMorgan Chase & Co

GLOBAL PRIVACY CODE (EEA)

The JPMC Global Code of Conduct expresses JPMC's commitment to conduct its business in accordance with high ethical standards and in accordance with applicable laws and JPMC policies, including with respect to the protection of personal information. This Privacy Code explains how JPMC will protect the personal information of its employees, customers, suppliers, business partners and related individuals in its role as a data controller. Capitalized terms have the meaning set out in Annex 1 (Definitions).

ARTICLE 1 – SCOPE, APPLICABILITY, AND IMPLEMENTATION

Scope

1.1 This Privacy Code applies to JPMC's global Processing of personal information as a Data Controller, with respect to (a) Customers, Suppliers, Business Partners, and other individuals in the context of its business activities and (b) Employees and their Dependents in the context of Employees' working relationship with JPMC, in each case where such personal information is subject to EEA Data Protection Law (or was subject to EEA Data Protection Law prior to the transfer of such personal information to a Group Company outside of the EEA) (respectively, CSB Information and Employee Information; together, **Personal Information**).

This Privacy Code applies to the Processing of Personal Information by electronic means or in systematically accessible paper-based filing systems.

The Privacy Code covers all types of Personal Information which JPMC Processes in the context of its business activities and employment relationships.

The Personal Information in the context of the employment relationships may include information such as: names and contact details, details of relationship with JPMC (e.g., contract terms and/or termination date of (former) employees or other temporary workers, position as a (former) member of the board), employment details (role, business activities and current and former employers) recruitment data (e.g., information contained in a resume, application status), human resources data (e.g., personal details, salary, performance reviews, information regarding family members/dependents, details of education and qualifications, and other information contained in a personnel file), and information collected in the context of security, authentication, investigations, fraud prevention, risk-management, and health and safety.

The Personal Information in the context of the provision of its business activities may include information such as: names and contact details, details of relationship with JPMC, operational and transaction data, communications records, information collected in the context of AML/KYC, client on-boarding, credit worthiness, loyalty programs and marketing and promotional activities, online interactions with JPMC (including electronic identifying data), and information collected in the context of security, authentication, investigations, fraud prevention, risk-management, financial crime, and health and safety.

Interaction with Local Law

1.2 Nothing in this Privacy Code will be construed to take away any rights and remedies that Individuals may have under applicable local law. This Privacy Code provides supplemental rights and remedies to Individuals only.

Interaction with Other Policies, Guidelines and Notices

1.3 This Privacy Code supplements other JPMC policies and standards including privacy policies, guidelines and notices that exist on the Effective Date. JPMC may further supplement this Privacy Code through policies, guidelines, and notices that are consistent with this Privacy Code. In case of conflicts, this Privacy Code takes precedence.

Binding Effect, Role of JPMC Germany

1.4 This Privacy Code is binding on JPMC. All Group Companies and Staff must comply with this Privacy Code. JPMorgan Chase & Co. has tasked J.P. Morgan AG (**JPMC Germany**) with the oversight, coordination and implementation of this Privacy Code. Annex 6 contains r a list of Legal Entities.

Effective Date

1.5 This Privacy Code has been adopted by JPMorgan Chase & Co. and will enter into force as of January 1, 2021 (**Effective Date**) and the parts of the Privacy Code relevant for Individuals will be published on the JPMC internet site and JPMC global intranet and will be made available to Individuals upon request. This Privacy Code will be implemented in the JPMC organization based on the timeframes specified in Article 17.

Scope extension to non-EEA Countries with similar transfer restrictions

1.6 JPMC may extend the scope of this Privacy Code to countries with data protection laws imposing data transfer restrictions similar to the data transfer restrictions under EEA Data Protection Law. The decision requires the prior approval of the Chief Privacy Officer and will be published on the JPMC internet site and JPMC global intranet.

Index

ARTICLE 2 – PROCESSING OF PERSONAL INFORMATION

Lawfulness and Purposes of Processing

2.1 JPMC will Process Personal Information lawfully. Lawful Processing means that JPMC will ensure that there is a valid legal basis for Processing of Personal Information under EEA Data Protection Law at all times, such as (a) the entering into or performance of a contract; (b) to comply with a legal obligation to which JPMC is subject; (c) to protect a vital interest of the Individual; (d) the legitimate interest of JPMC or a third party where these interests do not prejudice the interests or fundamental rights and freedoms of the Individual concerned; or (e) with the Individual's consent. Processing of Personal Information for the business purposes listed in Annex 2 can generally be based on one of these main legal bases, but remains subject to any applicable requirements and restrictions under EEA Data Protection Law.

JPMC may collect, use, or otherwise Process Personal Information only (i) for the applicable business purposes listed in Annex 2 (**Specified Business Purposes**); (ii) for a Secondary Purpose, subject to Article 2.2; and/or (iii) with the consent of the Individual to the Processing, subject to Articles 2.3 and 2.4, as applicable. JPMC may collect, use, or otherwise Process Special Categories of Information only (i) for the Specified Business Purposes or General Purposes listed in Annex 2 for Special Categories of Information and/or (ii) with the explicit consent of the Individual to the Processing, subject to Articles 2.3 and 2.4, as applicable.

Secondary Purposes

2.2 (i) Personal Information may be processed for a business purpose other than the Specified Business Purposes (**Secondary Purpose**) only if the Secondary Purpose is closely related to ('compatible' with) a Specified Business Purpose. Such Secondary Purposes include:

(a) transfer of the Personal Information to an Archive;

(b) internal audits or investigations;

(c) implementation of business controls and operational efficiency;

(d) IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);

(e) statistical, historical or scientific research;

(f) dispute resolution;

(g) legal or business consulting; or

(h) insurance purposes.

(ii) Depending on the sensitivity of the relevant Personal Information and whether use of the Personal Information for the Secondary Purpose has potential negative consequences for the individual, such use for a Secondary Purpose may require additional measures such as:

(a) limiting access to the Personal Information;

(b) imposing additional confidentiality requirements;

(c) taking additional security measures, including encryption or pseudonymization;

(d) informing the individual about the Secondary Purpose;

(e) providing an opt-out opportunity to the Individual; or

(f) obtaining the Individual's consent in accordance with Article 2.3 or Article 2.4 (if applicable).

Consent for Processing of Personal Information

2.3 Personal Information may be Processed based on the Individual's consent in the following circumstances:

(i) CSB Information may be Processed if the CSB Individual has given his or her consent to the Processing.

(ii) Except as provided below, Employee consent generally should not be used as a basis for Processing Employee Information.

(a) Employees may be asked to consent to Processing of Employee Information only if (a) none of the Business Purposes apply, (b) the Processing has no foreseeable adverse consequences for the Employee, and (c) the appropriate Privacy Lead has authorized the decision to seek Employee consent for the Processing.

(b) If an individual applies for employment or other work engagement with JPMC, JPMC may request the individual's consent to Process his/her Employee Information for purposes of evaluating his/her application.

In the event that a Business Purpose applies, but applicable law requires that JPMC also seek consent of the Individual for the Processing, JPMC will seek consent of the Individual to the relevant Processing to the extent required by applicable law.

Consent Process

2.4 When seeking an Individual's consent to Processing, JPMC must inform the Individual:

(i) of the purposes of the Processing for which consent is required;

(ii) which Group Company is responsible for the Processing;

(iii) of the potential consequences for the Individual of the Processing;

(iv) of the right to withdraw his or her consent at any time;

(v) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.

The Individual may deny or withdraw consent at any time. Upon withdrawal of consent, JPMC will discontinue Processing as soon as reasonably practical. 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 Information for other Business Purposes not based on consent after withdrawal.

ARTICLE 3 – PROCESSING OF PERSONAL INFORMATION FOR DIRECT MARKETING

Direct Marketing 3.1 JPMC's Processing of Personal Information 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) will be subject to this Article 3.

Consent for Direct Marketing (opt-in) 3.2 If applicable law so requires, JPMC shall send direct marketing communications to an Individual only with the Individual's prior opt-in consent. If applicable law does not require prior opt-in consent of the Individual, JPMC shall offer the Individual the opportunity to opt-out of such direct marketing communications.

Objection to Direct Marketing 3.3 If an Individual objects to receiving direct marketing communications from JPMC, or withdraws his or her consent to receive such communications, JPMC will take steps to refrain from sending further direct marketing communications as specifically requested by the Individual. JPMC will do so within the time period required by applicable law.

ARTICLE 4 – QUANTITY AND QUALITY OF PERSONAL INFORMATION

No Excessive Personal Information 4.1 JPMC shall restrict the Processing of Personal Information to Personal Information that is reasonably adequate for and relevant to the applicable Business Purpose. JPMC shall take reasonable steps to (i) delete or otherwise render beyond use (e.g., by scrambling) Personal Information that is not required for the applicable Business Purpose, and (ii) rectify Personal Information that is inaccurate.

Storage Period 4.2 JPMC generally shall retain Personal Information only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with applicable law, or as advisable in light of an applicable statute of limitations. JPMC may specify (e.g., in a

sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Information may be kept.

Promptly after the applicable storage period has ended, the Responsible Executive shall direct that the Personal Information be:

(i) securely deleted or destroyed in accordance with Article 4.1;

(ii) de-identified; or

(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Personal Information

4.3 Personal Information should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

'Privacy by Design and Default'

4.4 JPMC 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 technical and organizational steps to ensure that the requirements of this Article 4 are implemented, consistent with privacy by design and by default principles under applicable EEA Data Protection Laws, when implementing new systems and processes that Process Personal Information.

Accurate, Complete and Up-to-date Personal Information

4.5 It is the responsibility of Individuals to ensure that Personal Information that is provided by them to JPMC is accurate, complete and up-to-date.

Where JPMC requires an Employee to update his or her own Employee Information, JPMC shall remind him or her at least once a year to do so.

ARTICLE 5 – INFORMATION REQUIREMENTS FOR PERSONAL INFORMATION

Information Requirements

5.1 To the extent applicable, JPMC shall inform Individuals at the time when Personal Information is obtained through a privacy policy or notice of the following with respect to their Personal Information:

(i) the Business Purposes (including Secondary Purposes) for which their Personal Information is Processed;

(ii) which Group Company is responsible for the Processing as well as the contact information of the responsible Privacy Lead;

(iii) the categories of Third Parties to which the Personal Information is disclosed (if any), whether any such Third Party is covered by an Adequacy Decision and, if not, information on the data transfer mechanism as referred to in Article 9.5 (ii), (iv) or (v) as well as the means to get a copy thereof or access thereto; and

(iv) other relevant information, for example:

(a) the nature and categories of the Personal Information Processed;

(b) the period for which the Personal Information will be stored or (if not possible) the criteria used to determine this period;

(c) an overview of the rights of Individuals under this Privacy Code, how these can be exercised, including the right to obtain compensation;

(d) the existence of automated decision making referred to in Article 8 as well as meaningful information about the logic involved and potential negative consequences thereof for the Individual; or

(e) the source of the Personal Information (where the Personal Information has not been obtained from the Individual), including whether the Personal Information came from a public source.

Personal Information not Obtained from the Individual

5.2 Where Personal Information has not been obtained directly from the Individual, JPMC shall provide the Individual with the information as set out in Article 5.1:

(i) within a reasonable period after obtaining Personal Information but at the latest within one month, having regard to specific circumstances of the Personal Information Processed;

(ii) if Personal Information is used for communication with an Individual, at the latest at the time of the first communication with the Individual;

(iii) if a disclosure to another recipient is envisaged, at the latest when Personal Information is first disclosed.

Exceptions

5.3 The requirements of this Article 5 may be inapplicable if:

(i) the Individual already has the information as set out in this Article 5; or

(ii) Where Personal Information has not been obtained directly from the Individual,

(a) it would be impossible or would involve a disproportionate effort to provide the information to Individuals, in which case JPMC will take additional measures to mitigate potential negative consequences for the Individual, such as those listed in Article 2.2(ii);

(b) obtaining Personal Information is expressly laid down in applicable law; or

(c) the Personal Information must remain confidential subject to an obligation of professional secrecy regulated by applicable local law, including a statutory obligation of secrecy.

ARTICLE 6 – RIGHTS OF INDIVIDUALS

Right of Access 6.1 Every Individual has the right to request a copy of his or her Personal Information Processed by or on behalf of JPMC, and further, where reasonably possible, access to the information listed in Article 5.1.

Right to Rectification, Deletion, and Restriction 6.2 If the Personal Information is incorrect, incomplete, or not Processed in compliance with EEA Data Protection Law or this Privacy Code, the Individual has the right to have his or her Personal Information rectified, deleted or the Processing thereof restricted (as appropriate). In case the Personal Information has been made public by JPMC, and the Individual is entitled to deletion of the Personal Information, in addition to deleting the relevant Personal Information, JPMC shall take commercially reasonable steps to inform Third Parties that are Processing the relevant Personal Information or linking to the relevant Personal Information, that the Individual has requested the deletion of the Personal Information by such third parties.

Right to Object 6.3 The individual has the right to object to:

(i) the Processing of his or her Personal Information on grounds relating to his or her particular situation, unless JPMC can demonstrate prevailing compelling legitimate grounds for the Processing; and

(ii) receiving marketing communications on the basis of Article 3.3 (including any profiling related thereto).

Restrictions to Rights of Individuals 6.4 The rights of Individuals set out in Articles 6.1-6.3 above do not apply in one or more of the following circumstances:

(i) the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of JPMC;

(ii) the Processing is required by or allowed for a task carried out in the public interest, including in the areas 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 JPMC or others; or

(vi) in case a specific restriction of the rights of Individuals applies under EEA Data Protection Law.

The right of access as set out in Article 6.1 can only be restricted by the circumstances under (v) and (vi).

Procedure 6.5 An Individual should send his or her request to the contact indicated in the relevant privacy statement or notice. An Employee should send his or her request to the appropriate Privacy Lead. Individuals may also send their request to the Privacy Office via email to emea.privacy.office@jpmchase.com.

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

(i) specify the categories of Personal Information to which he or she is seeking access;

(ii) specify, to the extent reasonably possible, the system in which the Personal Information is likely to be stored;

(iii) specify the circumstances in which JPMC obtained the Personal Information;

(iv) provide proof of his or her identity when JPMC has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification;

(v) pay a fee to compensate JPMC for the reasonable costs relating to fulfilling the request provided JPMC can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character; and

(vi) in case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Information is incorrect, incomplete or not Processed in accordance with EEA Data Protection Law or this Privacy Code.

Response Period

6.6 Within one calendar month of JPMC receiving the request and any information necessary under Article 6.5, the contact person or the Privacy Office shall inform the Individual in writing or electronically (i) of JPMC's position with regard to the request and any action JPMC has taken or will take in response; (ii) a specification of the information necessary for JPMC to comply with the request in accordance with Article 6.5; or (iii) the ultimate date on which he or she will be informed of JPMC's position and the reasons for the delay, which shall be no later than two calendar months after the original one month period.

Denial of Requests

6.7 JPMC may deny an Individual's request if:

(i) the request does not meet the requirements of Articles 6.1-6.3 or meets the requirements of Article 6.4;

(ii) the request is not sufficiently specific;

(iii) the identity of the relevant Individual cannot be established by reasonable means, including additional information provided by the Individual; or

(iv) JPMC can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval.

Complaint

6.8 An Individual may file a complaint in accordance with Annex 5 and/or file a complaint or claim with the authorities or the courts in accordance with Article 13 if:

(i) the response to the request is unsatisfactory to the Individual (e.g., the request is denied);

(ii) the Individual has not received a response as required by Article 6.6; or

(iii) the time period provided to the Individual in accordance with Article 6.6 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 or she will receive a response.

No Requirement to Process Identifying Information

6.9 JPMC is not obliged to Process additional information in order to be able to identify the Individual for the sole purpose of facilitating the rights of the Individual under this Article 6.

ARTICLE 7 – OVERRIDING INTERESTS FOR PERSONAL INFORMATION

Overriding Interests

7.1 Certain obligations of JPMC or rights of Individuals may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) protect the legitimate business interests of JPMC including:

(a) the health, security or safety of Individuals;

(b) JPMC's intellectual property rights, trade secrets or reputation;

(c) the continuity of JPMC's business operations;

(d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or

(e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes;

(ii) prevent or investigate (including cooperating with law enforcement) suspected or actual fraud or violations of law, breaches of the terms of employment, or non-compliance with the JPMC Code of Conduct or other JPMC policies or procedures; or

(iii) otherwise protect or defend the rights or freedoms of JPMC, its Employees or other persons.

Exceptions in the Event of Overriding Interests

7.2 Except as provided below, one or more of the following obligations of JPMC or rights of the Individual may be set aside if an Overriding Interest exists:

(i) Article 2.1 (the requirement to Process Personal Information for specified purposes or closely related purposes); provided that the Article 2.1 requirements may be set aside with respect to Special Categories of Information only for the Overriding Interests listed in Article 7.1 (i) (a), (b), (c) and (e), (ii) and (iii);

(ii) Article 4.2 (data storage and deletion);

(iii) Articles 5.1 and 5.2 (information provided to Individuals);

(iv) Article 6 (rights of Individuals);

(v) Articles 9.3, 9.4 and 9.5(ii) (contracts with Third Parties); and

(vi) Article 10.2 (Staff access limitations and confidentiality requirements).

Consultation with Chief Privacy Officer

7.3 Setting aside obligations of JPMC or rights of Individuals based on an Overriding Interest requires prior consultation with the Privacy Office. The Privacy Office shall document its advice. If application of Article 7.1 – 7.2 conflicts with EEA Data Protection Law, this conflict will be handled in accordance with Article 15.1.

Information to Individual

7.4 Upon request of the Individual, JPMC shall inform the Individual of the Overriding Interest for which obligations of JPMC or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 5.1 or 6.1-6.3, in which case the request shall be denied.

ARTICLE 8 – AUTOMATED DECISION MAKING USING PERSONAL INFORMATION

Automated Decisions

8.1 Automated tools may be used to make decisions about Individuals, but decisions with a significant negative outcome for the Individual may not be based solely on the results provided by the automated tool. This restriction does not apply if:

(i) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation to which JPMC is subject; or

(ii) the decision is made by JPMC for purposes of:

(a) with respect to CSB Individuals, entering into or performing a contract (including assessing creditworthiness or eligibility or for fraud prevention purposes), provided the underlying request leading to a decision by JPMC was made by the CSB Individual (e.g., where automated tools are used to filter applications for financial products or services); or

(b) with respect to Employees, (1) entering into or performing a contract; or (2) managing the employment relationship, provided the underlying request leading to a decision by JPMC was made by the Employee (e.g., where automated tools are used to filter job applications); or

(iii) the decision is made based on the explicit consent of the Individual.

Items (ii) and (iii) only apply if suitable measures are taken to safeguard the legitimate interests of the Individual (e.g., the Individual has been provided with an opportunity to express his or her point of view).

The requirements set out in Articles 2.3 and 2.4 apply to the requesting, denial or withdrawal of Individual consent.

ARTICLE 9 – TRANSFERS OF PERSONAL INFORMATION TO THIRD PARTIES OR JPMC PROCESSORS

Transfer to Third Parties

9.1 This Article sets forth requirements concerning the transfer of Personal Information from JPMC to a Third Party or a JPMC Processor. Note that a transfer of Personal Information includes situations in which JPMC discloses Personal Information to a Third Party or JPMC Processor (e.g., in the context of corporate due diligence) or where JPMC provides remote access to Personal Information to a Third Party or JPMC Processor.

Categories of Third Parties

9.2 There are two categories of Third Parties involved in Processing of Personal Information:

(i) **Third Party Processors**: these are Third Parties that Process Personal Information solely on behalf of JPMC as a Data Controller and at its direction (e.g., Third Parties that Process applications made by Customers or Third Parties that Process Employee payroll on behalf of JPMC).

(ii) **Third Party Controllers**: these are Third Parties that Process Personal Information and determine the purpose and means of the Processing (e.g., JPMC Business Partners that provide their own goods or services directly to Customers).

Transfers to Third-Party Processors

9.3 JPMC may use Third Party Processors to Process Personal Information, subject to the following requirements:

(i) JPMC may transfer Personal Information to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 2.2 or purposes for which the Individual has provided consent in accordance with Article 2.3).

(ii) Third Party Processors may Process Personal Information only if they have a validly entered into written or electronic contract with JPMC (**Processor Contract**). The Processor Contract must in any event include the following obligations:

(a) The Third Party Processor shall Process Personal Information only for the purposes authorized by JPMC and in accordance with JPMC's documented instructions, including on transfers of Personal Information to any Third Party Processor not covered by an Adequacy Decision, unless the Third Party Processor is required to do so under mandatory requirements applicable to the Third Party Processor and notified to JPMC;

(b) The Third Party Processor shall keep the Personal Information confidential and shall impose confidentiality obligations on Staff with access to Personal Information;

(c) The Third Party Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Information;

(d) The Third Party Processor shall only permit subcontractors to Process Personal Information in

connection with its obligations to JPMC (a) with the prior specific or generic consent of JPMC and (b) based on a validly entered into written or electronic contract with the subcontractor, which imposes data protection obligations that shall be no less protective than those imposed on the Third Party Processor under the Processor Contract and provided that the Third Party Processor remains liable to JPMC for the performance of the subcontractor in accordance with the terms of the Processor Contract. If JPMC provides generic consent for involvement of subcontractors, the Third Party Processors shall provide notice to JPMC of any changes in its subcontractors and will provide the Customer the opportunity to object to such changes based on reasonable grounds;

(e) JPMC should be able to verify the security measures taken by the Third Party Processor (a) by an obligation of Third Party Processor to submit its relevant information processing facilities to audits and inspections by JPMC, a Third Party on behalf of JPMC, or any relevant public authority; or (b) by means of a statement issued by a qualified independent third party assessor on behalf of Third Party Processor certifying that the information processing facilities of the Third Party Processor used for the Processing of the Personal Information comply with the requirements of the Processor Contract;

(f) The Third Party Processor shall promptly inform JPMC of an Information Security Breach involving Personal Information;

(g) The Third Party Processor shall deal promptly and appropriately with (a) requests for information necessary to demonstrate compliance of the Third Party Processor with its obligations under the Processor Contract and will inform JPMC if any instructions of JPMC in this respect violate EEA Data Protection Law; (b) requests and complaints of Individuals as instructed by JPMC; and (c) requests for assistance of JPMC as reasonably required to ensure compliance of the Processing of the Personal Information with EEA Data Protection Law; and

(h) Upon termination of the Processor Contract, the Third Party Processor shall, at the option of JPMC, return the Personal Information and copies thereof to JPMC or shall securely delete such Personal Information, except to the extent the Processor Contract or applicable law provides otherwise.

Transfers to Third Party Controllers

9.4 JPMC may permit Third Party Controllers (other than government agencies) to Process Personal Information transferred by JPMC if they have validly entered into written or electronic contract with JPMC. In the contract, JPMC shall seek where appropriate to contractually protect the privacy protection interests of Individuals when Personal Information is Processed by Third Party Controllers. All such contracts

shall be drafted consistent with JPMC contracting guidelines. This provision does not apply in case of incidental transfers of Personal Information to a Third Party Controller, such as when a reference is provided for an Employee or in case of sending details for a hotel booking.

Transfers to Third Parties outside the EEA that are not Covered by Adequacy Decisions

9.5 JPMC may permit Personal Information that is collected originally in connection with activities of a Group Company that is located in the EEA or covered by an Adequacy Decision to be transferred to a Third Party that is located outside the EEA and not covered by an Adequacy Decision if:

(i) the Third Party has been certified under an approved mechanism that is recognized under applicable Data Protection Law as providing an adequate level of data protection, such as the EU-US Privacy Shield;

(ii) the Third Party is a Processor and has implemented Binding Corporate Rules for Processors or a similar transfer control mechanism that is recognized under applicable Data Protection Law as providing appropriate safeguards;

(iii) a contract has been concluded between JPMC and the relevant Third Party that (a) provides for safeguards at a similar level of protection as that provided by this Privacy Code; or (b) that is recognized under applicable Data Protection Law as providing appropriate safeguards;

(iv) the transfer is necessary for the performance of a contract with the Individual or otherwise subject to an applicable derogation under applicable law (e.g., necessary to protect a vital interest of the Individual, necessary for the establishment, exercise, or defense of a legal claim, etc.);

(v) the transfer is necessary for the performance of a task carried out to comply with a legal obligation to which the relevant Group Company is subject; or

(vi) the Individual has given his or her explicit consent to the transfer, in accordance with Article 2.4 and applicable law.

Items (v) and (vi) above require the prior approval of the Chief Privacy Officer.

Transfers to JPMC Processors

9.6 JPMC may at any time involve JPMC Processors, provided they have a validly entered into written or electronic contract with the Group Company being the Data Controller of the relevant Personal Information, which contract must in any event include the provisions set out in Article 9.3(ii).

ARTICLE 10 – SECURITY AND CONFIDENTIALITY REQUIREMENTS

Information Security

10.1 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, JPMC shall take appropriate technical, physical and

organizational measures to protect Personal Information from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, JPMC has developed and implemented the JPMC IT security policies and other sub-policies and guidelines relating to the protection of Personal Information.

Staff Access and Confidentiality 10.2 JPMC shall provide JPMC Staff access to Personal Information only to the extent necessary to serve the applicable Business Purpose and to perform their job. JPMC shall impose confidentiality obligations on Staff with access to Personal Information.

Information Security Breach Notification Requirement 10.3 JPMC shall document any Information Security Breaches, comprising the facts relating to the Information Security Breach, its effects and the remedial actions taken, which documentation will be made available to the Lead SA and other SAs competent to audit under Article 12.2 upon request. Group Companies shall inform JPMC Germany of an Information Security Breach without delay. JPMC shall notify the appropriate SA(s) or affected Individuals as soon as reasonably possible following its determination that an Information Security Breach has occurred to the extent such reporting is required by EEA Data Protection Law. JPMC shall respond promptly to inquiries of affected Individuals relating to such Information Security Breach.

JPMC may delay or refrain from providing such notifications if otherwise prohibited, such as if a law enforcement official or a supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security or the relevant industry sector. In this case, notification shall be delayed or withheld as instructed by such law enforcement official or supervisory authority.

ARTICLE 11 – PRIVACY GOVERNANCE, POLICIES AND PROCEDURES

Privacy Governance Structure 11.1 JPMC shall maintain a privacy governance program as described in Annex 4

Procedures and Guidelines 11.2 JPMC shall develop and implement policies and procedures to comply with this Privacy Code.

System Information 11.3 JPMC shall maintain records of its data processing activities in compliance with EEA Data Protection Law.. A copy of this information will be provided to the SA competent for JPMC upon request.

Data Protection Impact Assessment 11.4 JPMC shall maintain a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Information, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used (Data Protection Impact Assessment). Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by JPMC, the Processing still presents a residual high risk for the rights and freedoms of Individuals,

the SA competent for JPMC will be consulted prior to such Processing taking place.

Staff Training 11.5 JPMC shall provide training on the obligations and principles laid down in this Privacy Code, related confidentiality and security obligations to Staff who Process Personal Information or are involved in the development of tools used to Process Personal Information.

ARTICLE 12 – MONITORING AND AUDITING COMPLIANCE

Internal Audits 12.1 JPMC Internal Audit shall audit business processes and procedures that involve the Processing of Personal Information for compliance with this Privacy Code, including methods of ensuring that corrective actions will take place. The audit process will cover all applicable areas of compliance with the Privacy Code. The audits shall be carried out in the course of the regular activities of JPMC Internal Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article conducted by an accredited external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Leads shall be informed of the results of the audits. Any violations of the Privacy Code identified in the audit report will be reported to the Responsible Executive. A copy of the audit results related to compliance with this Privacy Code will be provided upon request to the Lead SA and any other SA with authority to audit JPMC pursuant to Article 12.2.

SA Audit 12.2 The Lead SA may request an audit of the facilities used by JPMC for the Processing of Personal Information for compliance with this Privacy Code. In addition, the SA of the EEA Country at the origin of a data transfer under this Privacy Code will be authorized to audit the relevant data transfer for compliance with this Privacy Code.

Annual Privacy Report 12.3 The Chief Privacy Officer shall produce an annual privacy report for the **Global Operating Committee** of JPMorgan Chase & Co. on compliance with this Privacy Code, privacy protection risks and other relevant issues.

Each Privacy Lead shall provide information relevant to the report to the Chief Privacy Officer.

Mitigation 12.4 JPMC shall, if so indicated, ensure that adequate steps are taken to address breaches of this Privacy Code identified during the monitoring or auditing of compliance pursuant to this Article.

ARTICLE 13 – ENFORCEMENT RIGHTS OF INDIVIDUALS

Rights of Individuals

13.1 This Article 13 provides rights to Individuals to enforce commitments made by JPMC under this Privacy Code with respect to its Processing of Personal Information.

The rights contained in this Privacy Code are in addition to, and shall not prejudice, any other rights or remedies that an Individual may otherwise have by law.

Individuals are encouraged to first follow the complaints procedure set forth in Annex 5 of this Privacy Code before filing any complaint or claim with a competent SA or court.

If JPMC violates the Privacy Code with respect to the Personal Information of an Individual (**Affected Individual**) covered by this Privacy Code, the Affected Individual can as a third party beneficiary enforce any claim as a result of a breach of Articles 1.5, 2 – 6, 7.3, 7.4, 8, 9, 10, 12.2, 13, 14.2, 14.3, 15.3 and Annex 5 in accordance with Article 13.2.

Local Law and Jurisdiction

13.2 In case of a violation of this Privacy Code, the Affected Individual may, at his/her choice, submit a complaint or a claim under Article 13.1 to:

(i) the Lead SA or the courts: in Germany, against JPMC Germany;

(ii) the SA in the EEA Country where (a) the Individual has his/her habitual residence or place of work, or (b) the infringement took place, against the Group Company that is the Data Controller of the relevant Personal Information or JPMC Germany; or

(iii) the courts in the EEA country (a) where the Individual has his or her habitual residence, or (b) where the Group Company being the Data Controller of the relevant Personal Information is established, against the Group Company being the Data Controller of the relevant Personal information or JPMC Germany.

The Group Company against which a complaint or claim is brought (relevant Group Company), may not rely on a breach by another Group Company or a Third Party Processor of its obligations to avoid liability except to the extent any defense of such other Group Company or Third Party Processor would also constitute a defense of the relevant Group Company.

The SAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Individual will not prejudice the substantive or procedural rights he/she may have under applicable law.

Right to Claim Damages

13.3 In case an Individual has a claim under Article 13.1, such Individual shall be entitled to compensation of material and immaterial damages suffered by an Individual resulting from a violation of this Privacy Code to the extent provided by applicable EEA law.

Burden of Proof in Respect of Claim for

13.4 In case an Individual brings a claim for damages under Article 13.2, it will be for the Individual to demonstrate that he/she has suffered the relevant damages and to establish facts which show it is plausible that

Damages the damage has occurred because of a violation of this Privacy Code. It will subsequently be for the relevant Group Company to prove that the damages suffered by the Individual due to a violation of this Privacy Code are not attributable to JPMC or a Processor or to assert other applicable defenses.

Mitigation 13.5 JPMC Germany shall ensure that adequate steps are taken to address violations of this Privacy Code by a Group Company.

Law Applicable to this Code 13.6 This Code shall be governed by and interpreted in accordance with the laws of Germany.

ARTICLE 14 – SANCTIONS, REDRESS, AND COOPERATION

Sanctions for Non-compliance 14.1 Non-compliance of Employees with this Privacy Code may result in disciplinary action in accordance with JPMC policies and local law, up to and including termination of employment.

Mutual Assistance and Redress 14.2 All Group Companies shall 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 SA or public authority.

The Group Company that receives a request, complaint or claim from an Individual is responsible for promptly notifying the appropriate Privacy Lead thereof and handling any communication with the Individual regarding his/her request, complaint or claim as instructed by the appropriate Privacy Lead except where circumstances dictate otherwise.

Advice of the SAs 14.3 JPMC shall take into account and abide by the advice of the Lead SA and the SAs competent pursuant to Article 12.2 issued on the interpretation and application of this Privacy Code.

ARTICLE 15 – CONFLICTS BETWEEN THIS PRIVACY CODE AND APPLICABLE LOCAL LAW

Conflict Between Privacy Code and Local Law 15.1 Where there is a conflict between applicable local law of a non-EEA Country and this Privacy Code, including where a legal requirement to transfer Personal Information conflicts with EEA Data Protection Law, the relevant Responsible Executive shall promptly consult with the Chief Privacy Officer to determine how to comply with this Privacy Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company. The Chief Privacy Officer may seek the advice of the Lead SA or another competent public authority

New Conflicting Legal 15.2 The relevant Responsible Executive, in consultation with the legal department, shall promptly inform the Chief Privacy Officer of any new

Requirements

legal requirement of a non-EEA country that may interfere with JPMC's ability to comply with this Privacy Code.

Requests for Disclosure of Personal Information

15.3 Subject to the following paragraph, JPMC shall promptly inform the Lead SA if JPMC becomes aware that applicable local law of a non-EEA country is likely to have a substantial adverse effect on the protection offered by this Privacy Code, including if JPMC receives a legally binding request for disclosure of Personal Information from a law enforcement authority or state security body of a non-EEA country (**Disclosure Request**). Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure.

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, JPMC will request the relevant authority to waive this prohibition and will document that it has made this request, which documentation will be provided to the Lead SA upon request. In any event, JPMC will on an annual basis provide to the Lead SA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by applicable law.

In any event, any transfers by JPMC of Personal Information 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.

This Article does not apply to requests received from other government agencies in the normal course of the business activities of JPMC (such as subpoenas or court orders in connection with civil litigation, or information requests from banking or financial supervisory authorities with regulatory oversight over JPMC), which JPMC can continue to provide in accordance with applicable law.

ARTICLE 16 – CHANGES TO THIS PRIVACY CODE

Approval of Changes

16.1 Any changes to this Privacy Code require the prior approval of the **Chief Privacy Officer** and shall thereafter be communicated to the Group Companies.

Effective Time of Changes

16.2 Any change shall enter into force with immediate effect after it is approved in accordance with Article 16.1 and published on the JPMC website.

Governing Version

16.3 Any request, complaint or claim of an Individual involving this Privacy Code shall be judged against the version of this Privacy Code as it is in force at the time the request, complaint or claim is made.

Reporting of Material Changes to Lead SA

16.4 The Chief Privacy Officer shall promptly inform the Lead SA of changes to this Privacy Code that have a material impact on the protection offered by this Privacy Code or the Privacy Code itself and will be responsible for coordinating JPMC’s responses to questions via the

Lead SA in respect thereof. The Chief Privacy Officer shall inform the appropriate Privacy Leads of the effect of such responses. Other non-material changes, as well as any updates to the list of Group Companies subject to this Privacy Code, will be notified by the Chief Privacy Officer to the Lead SA on a yearly basis, including a brief explanation of the reasons justifying the update.

ARTICLE 17 – TRANSITION PERIODS

Transition Period for New Group Companies

17.1 Any entity that becomes a Group Company after the Effective Date shall comply with this Privacy Code within two years of becoming a Group Company. During this transition period, no Personal Information will be transferred under this Privacy Code until (i) the relevant Group Company has achieved compliance with the Privacy Code or (ii) an alternative data transfer mechanism under EEA Data Protection Law has been implemented, such as standard contractual clauses.

Transition Period for Divested Entities

17.2 A Divested Entity (or specific parts thereof) will remain covered by this Privacy Code after its divestment for such period as is required by JPMC to disentangle the Processing of Personal Information relating to such Divested Entity.

Transition Period for IT Systems

17.3 Where implementation of this Privacy Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition Period for Existing Agreements

17.4 Where there are existing agreements with Third Parties that are affected by this Privacy Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Contact Details

JPMC Privacy Office

emea.privacy.office@jpmchase.com

ANNEX 1 — DEFINITIONS

Adequacy Decision	ADEQUACY DECISION shall mean a decision issued by the European Commission under EEA Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.
Archive	ARCHIVE shall mean a collection of Personal Information that is no longer necessary to achieve the purposes for which the Personal Information originally was collected or that is no longer used for general business activities, but is used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An Archive includes any Personal Information set that can no longer be accessed by any Employee other than the system administrator.
Article	ARTICLE shall mean an article in this Privacy Code.
Authority	AUTHORITY shall have the meaning set forth in Article 15.4.
Binding Corporate Rules	BINDING CORPORATE RULES shall mean a privacy policy of a group of undertakings which, under applicable local law, is considered to provide an adequate level of protection for the transfer of Personal Information within that group of undertakings.
Business Partner	BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or has had a business relationship or strategic alliance with JPMC (e.g., joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE shall mean any Specified Business Purpose or Secondary Purpose.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer as referred to in Annex 4.
Children	CHILDREN shall mean Individuals under thirteen (13) years of age.
CSB Individual	CSB INDIVIDUAL shall mean any individual (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Information is Processed by JPMC as a Data Controller.

CSB Information

CSB INFORMATION shall have the meaning set forth in Article 1.1 above. This definition does not cover the Processing of Personal Information of Employees in the context of their employment relationship with JPMC unless and to the extent such Employee is a Customer of JPMC.

Customer

CUSTOMER shall mean any person, private organization, or government body that purchases, may purchase or has purchased a product or service from JPMC.

Data Controller

DATA CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Information.

Data Protection Impact Assessment (DPIA)

DATA PROTECTION IMPACT ASSESSMENT (DPIA) shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Information, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain:

(i) a description of:

(a) the scope and context of the Processing;

(b) the Business Purposes for which Personal Information is Processed;

(c) the specific purposes for which Special Categories of Information are Processed;

(d) categories of Personal Information recipients, including recipients not covered by an Adequacy Decision; and

(e) Personal Information storage periods.

(ii) an assessment of:

(a) the necessity and proportionality of the Processing;

(b) the risks to the privacy rights of Individuals; and

(c) the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Information.

Dependent

DEPENDENT shall mean the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee.

Disclosure Request

DISCLOSURE REQUEST shall have the meaning set forth in Article 15.4.

Divested Entity

DIVESTED ENTITY shall mean the divestment by JPMC of a

	Group Company or business by means of: (i) a sale of shares that results in the divested Group Company no longer qualifying as a Group Company; and/or (ii) a demerger, sale of assets, or any other manner or form.
EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein and for purposes of this Privacy Code, Switzerland, Jersey, and Guernsey.
EEA Country	EEA COUNTRIES (European Economic Area Countries) shall mean each country part of the EEA.
EEA Data Protection Law	EEA DATA PROTECTION LAW shall mean the provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.
Effective Date	EFFECTIVE DATE shall mean the date on which this Privacy Code becomes effective as set forth in Article 1.5.
Employee	EMPLOYEE shall mean the following individuals: (i) an employee, job applicant or former employee of JPMC including temporary workers working under the direct supervision of JPMC (e.g., independent contractors and trainees). This term does not include people working at JPMC as consultants or employees of Third Parties providing services to JPMC; and (ii) a (former) executive or non-executive director of JPMC or (former) member of the supervisory board or similar body to JPMC.
Employee Information	EMPLOYEE INFORMATION shall mean any Personal Information of an Employee (and his or her Dependents) Processed in the context of their (former) employment relationship with JPMC. This definition does not cover the Processing of Employee Information in the Employee's capacity as a customer of JPMC.
General Counsel	GENERAL COUNSEL shall mean the General Counsel of JPMorgan Chase & Co.
Group Company	GROUP COMPANY shall mean JPMorgan Chase & Co. and any company or legal entity of which JPMorgan Chase & Co. 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 a liaison and/or relationship exists.
Head of Compliance	HEAD OF COMPLIANCE shall mean the Head of Compliance of JPMorgan Chase & Co.
Individual	INDIVIDUAL shall mean any CSB Individual or Employee whose Personal Information is Processed by JPMC.
Information Security Breach	INFORMATION SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Information that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Individual. An Information Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Information by an Employee of JPMC or Third Party Processor or an individual acting under their respective authority, if: (i) the acquisition, access, or use of Personal Information was in good faith and within the course and scope of the employment or professional relationship of such Employee or other individual; and (ii) the Personal Information is not further acquired, accessed, used or disclosed by any person.
JPMC	JPMC shall mean JPMorgan Chase & Co. and its Group Companies.
JPMC Germany	JPMC GERMANY shall mean J.P. Morgan AG.
JPMC Processor	JPMC PROCESSOR shall mean any Group Company that Processes Personal Information on behalf of another Group Company being the Data Controller.
JPMorgan Chase & Co.	JPMorgan Chase & Co. shall mean JPMorgan Chase & Co., having its registered seat in NY, U.S.
Lead SA	LEAD SA shall mean the SA of Hesse, Germany.
Organizational Unit	ORGANIZATIONAL UNIT shall mean each business unit and staff function of JPMC.
Overriding Interest	OVERRIDING INTEREST shall have the meaning set forth in Article 8.

Personal Information	PERSONAL INFORMATION shall have the meaning set forth in Article 1.1.
Privacy Code	PRIVACY CODE shall mean this Privacy Code.
Privacy Council	PRIVACY COUNCIL shall mean the council referred to in Annex 4.
Privacy Lead	PRIVACY LEAD shall mean a Privacy Lead appointed by the Chief Privacy Officer pursuant to Annex 4.
Privacy Office	PRIVACY OFFICE shall have the meaning set forth in Annex 4.
Processing	PROCESSING shall mean any operation that is performed on Personal Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission, transfer, or deletion of Personal Information.
Processor Contract	PROCESSOR CONTRACT shall have the meaning set forth in Article 9.3(ii).
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean the lowest-level JPMC business executive or the non-executive general manager of a JPMC business function/unit who has primary budgetary ownership of the relevant Processing.
SA	SA shall mean any supervisory authority of one of the countries of the EEA.
Secondary Purpose	SECONDARY PURPOSE shall have the meaning set forth in Article 2.1.
Special Categories of Information	SPECIAL CATEGORIES OF INFORMATION shall mean Personal Information that reveals 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 information, biometric information, addictions, sex life, criminal convictions or offenses, or social security numbers issued by the government.
Specified Business Purposes	SPECIFIED BUSINESS PURPOSES shall have the meaning set forth in Article 2.1.
Staff	STAFF shall mean all Employees and other persons acting under the direct authority of JPMC who Process Personal

	Information as part of their respective duties or responsibilities towards JPMC using JPMC information technology systems or working primarily from JPMC's premises.
Supplier	SUPPLIER shall mean any Third Party that provides goods or services to JPMC (e.g., an agent, consultant or vendor).
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or public authority) outside JPMC.
Third Party Controller	THIRD PARTY CONTROLLER shall have the meaning set forth in Article 9.2(ii).
Third Party Processor	THIRD PARTY PROCESSOR shall have the meaning set forth in Article 9.2(i).

Interpretations

INTERPRETATION OF THIS PRIVACY CODE:

(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 this Privacy Code;

(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 this Privacy Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Privacy Code or that other document; and

(vii) a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2 — Specified Business Purposes

A. Specified Business Purposes of Processing CSB Information

1. AML/KYC (pre-contractual Customer checking)

Fulfilling anti-money laundering and "know your customer" requirements for the purposes of pre-contractual Customer and CSB Individual checking and vetting, in order to protect JPMC and Customers as well as to comply with regulatory and legal obligations.

2. Client on-boarding (not including those matters in Section 1 above)

Assessment and acceptance of a Customer, conclusion and execution of agreements with a Customer. This purpose includes Processing of Personal Information that is necessary in connection with the assessment and acceptance of Customers, including confirming and verifying a Customer's identity (this may involve the use of a credit reference agency or other Third Parties) assessing product suitability, financial and investment advice, and conducting due diligence, screening against publicly available government and/or law enforcement agency sanctions lists (but not including those matters in Section 1 above). This activity also includes the Processing of Personal Information in connection with the execution of agreements.

3. Credit worthiness

Processing for the purpose of contractual, compliance and legal checks to assess credit worthiness of Customers, Suppliers and Business Partners including: credit assessment (including setting credit limits); assessment of credit risk and rating; credit approvals; disclosures to credit reference agencies; and financial and investment advice related to the giving or receiving of credit, but not including profiling or automated decision-making in Section 8 below.

4. Employment-related purposes

Human resources and personnel management. This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing employment matters, e.g., management and administration of recruiting, outplacement, employability, leave and other absences, compensation and benefits (including pensions), payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, disciplinary and grievance matters, and Employee communications;

Business process execution, internal management, and management reporting. This purpose addresses activities such as scheduling work, recording time, managing company and Employee assets (including the IT systems and infrastructure), provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, finance and accounting, management reporting and analysis, implementing business controls, and managing and using Employee directories, managing mergers, acquisitions and divestitures, Archive and insurance purposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution;

Health, safety, security and integrity. This purpose addresses activities such as those involving the protection of the interests of JPMC, its Employees and customers and the sector in which JPMC operates, including the screening and monitoring of Employees before and during employment, including the screening against publicly available government and/or law

enforcement agency sanctions lists and other third-party data sources, the detecting, preventing, investigating and combating (attempted) fraud and other criminal or objectionable conduct, including the use of and participation in JPMC's incident registers and sector warning systems, occupational health and safety, the protection of company and Employee and customer assets, and the authentication of Employee status and access rights;

Organizational analysis and development, management reporting and acquisition and divestitures. This purpose addresses various activities, such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Information for management reporting and analysis;

Compliance with law. This purpose addresses Processing of Employee Information necessary for the performance of a task carried out to comply with a legal obligation to which JPMC is subject, and the disclosure of Employee Information to government institutions and supervisory authorities, including tax and other competent authorities for the sector in which JPMC operates;

Protecting the vital interests of Employees. This purpose addresses Processing necessary to protect the vital interests of an Employee; or

Permitted Processing with respect to Dependents. This purpose addresses Processing of Personal Information of Dependents of an employee if:

- the Personal Information was provided with the consent of the Employee or the Dependent;
- Processing of the Personal Information is reasonably necessary for the performance of a contract with the Employee; or
- the Processing is required or permitted by applicable local law.

5. Fraud Prevention/investigation/security

Fraud prevention. This purpose includes safeguarding the security and integrity of the financial sector, in particular the detecting, preventing, investigating and combating (attempted) criminal or other fraudulent conduct, misconduct, or market abuse directed against JPMC, Customers or other Customers, including the use of and participation in JPMC's incident registers and sector warning systems;

Health, safety, security and integrity. This purpose includes the protection of the interests of JPMC and its Customers, including activities such as those involving health and safety, the protection of JPMC and Employee assets including the operation and support of information technology assets, and the authentication of Customer, Supplier or Business Partner status and access rights (such as required screening activities for access to JPMC's premises or systems);

Business process execution. This purpose includes the management of company assets, including the IT systems and infrastructure; provision of central processing facilities for efficiency purposes; or

Protection of the vital interests of individuals. This purpose addresses Processing necessary to protect the vital interests of an individual.

6. Marketing/Prospecting

This purpose includes activities such as promoting contact with prospective Customers, Suppliers and Business Partners, and those where there is no existing business relationship,

collection of Personal Information through JPMC websites, and the development, execution and analysis of marketing strategies.

7. Product/Service implementation

This purpose includes Processing of Personal Information for the development and improvement of JPMC products and/or services, research and development, as well as for data security and fraud prevention purposes (for the purposes of product improvement/development). In certain cases, this Processing may involve automated decision-making, which shall be conducted in accordance with Article 8.

8. Provision of product/service

Conclusion and execution of agreements with Suppliers and Business Partners. This purpose addresses the Processing of Personal Information necessary to conclude and execute agreements with Suppliers and Business Partners, including required screening activities (e.g., for access to JPMC's premises or systems) and to record and financially settle delivered services, products and materials to and from JPMC;

Execution of agreements with a Customer including performance of agreements; legal or business consulting; debt collection and management; payments to be made to JPMC by Customers under commercial agreements; or

Relationship management. This purpose includes activities related to existing business relationships such as maintaining contact with existing Customers, Suppliers and Business Partners, account management, management of relationships with third party intermediaries, customer service, recalls, complaints management; collection of Personal Information through JPMC websites, and the development, execution and analysis of market surveys.

9. Audit, compliance, risk management and reporting, and legal purposes

Compliance with law and regulation. This purpose addresses Processing of Personal Information necessary for the performance of a task carried out to comply with a legal or regulatory obligation to which JPMC is subject, including the disclosure of Personal Information to government institutions or supervisory authorities, including tax authorities, including in relation to the prevention of money laundering, financing of terrorism and other crimes, customer due diligence and the duty of care towards Customers (e.g. credit monitoring) and the disclosure of Personal Information to government institutions and supervisory authorities, including tax authorities, in relation thereto; regulatory relationship management; monitoring and surveillance for compliance and regulatory reasons; protecting JPMC, Individuals, Customers, or Business Partners including preventing, preparing for or engaging in dispute resolution and whistleblowing;

Risk management and reporting. This purposes includes internal management and management reporting, such as risk and control management reporting, and conduct reporting; processing Personal Information for management reporting and analysis; implementing business controls; risk management; incident management and reporting;

Audit. This purpose includes processing for the purposes of internal and external audits or investigations; conducting audits and investigations.

Business process execution: This purpose includes Processing necessary to maintain and run a financially viable organization in accordance with law and regulation: finance and accounting; management of books and records, managing mergers, acquisitions and divestitures; archive and insurance purposes for JPMC.

10. Corporate or external relations

Corporate and community affairs. This purpose includes processing to enable and facilitate corporate and community programmes such as advertising, brand and media management, sponsorship and events.

Investor relations and governmental affairs. This purpose includes processing: to manage records about investors in JPMC, to prepare filings and reports for the purposes of complying with investment and listing rules, and for the management of relationships with governmental representatives and public officials.

B. Business Purposes for Processing Special Categories of Information

1. Specified Business Purposes for Processing Special Categories of Information

The following categories of Special Categories of Information may be collected, used or otherwise Processed for one (or more) of the purposes specified below:

(i) **Racial or ethnic information** (which in some countries includes photos and video images of individuals): JPMC may process photos (e.g., a copy of a passport containing a photo) and video images for the protection of JPMC, Customer, and Employee assets; site access and security reasons; assessment and acceptance of Customers, including

(a) **with respect to CSB Individuals**, the identification and authentication of Customers (including confirming and verifying the identity of relevant CSB Individuals); Supplier or Business Partner status and access rights; and to verify and confirm advice or record decisions made in the course of business for future reference (e.g., when CSB Individuals participate in video conferencing which is recorded); and

(b) **with respect to Employees**, screening and monitoring of Employees before and during employment; to verify and confirm advice or record decisions made in the course of business for future reference (e.g., when Employees participate in video conferencing which is recorded); monitoring and investigation of conduct for disciplinary, legal and regulatory purposes; photos for site access and security reasons and for inclusion in Employee directories; supporting workplace diversity programs to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant racial or ethnic Employee Information allows for an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection against the relevant Processing; and for administering Employee affinity groups.

(ii) **Criminal information** (including Personal Information relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior, or suspected criminal behavior), may be processed as necessary

(a) **with respect to CSB Individuals**, for assessment and acceptance of Customers, including the identification and authentication of Customers (including confirming and verifying the identity of relevant CSB Individuals); the execution of an agreement with Customers; and to protect the interests of JPMC, its Employees and Customers and for the use of and the participation in JPMC's incident registers and sector warning systems; and

(b) **with respect to Employees**, for assessing an application by an Employee, to make a decision about the Employee, or provide a service to the Employee; and protecting the interests of JPMC, its Employees, customers, and the sector in which JPMC operates, with respect to criminal offences that have been or, given the relevant circumstances, are suspected to be or have been, committed against JPMC, its Employees, customers or other companies in the sector in which JPMC operates, and for screening and monitoring of Employees before and during employment; including the use of and participation in JPMC's incident registers and sector warning systems.

(iii) **Physical or mental health information**: May be processed as necessary

(a) **with respect to CSB Individuals**, for the assessment and acceptance of a Customer, the execution of an agreement with a Customer, and compliance with JPMC's duty of care towards Customers including vulnerable customers; and

(b) **with respect to Employees**, including any opinion of physical or mental health and Employee Information relating to disabilities and absence due to illness or pregnancy, for the purposes of providing health services to an Employee, provided that the relevant health Employee Information is processed by or under the supervision of a health professional who is subject to professional confidentiality requirements; administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee; accommodating persons with a disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Special Categories of Information allows for an objective determination that an Employee belongs to the relevant category and the Employee has not filed a written objection against the relevant Processing; reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity; for screening and monitoring of Employees before and during employment and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities; and providing facilities in the workplace to accommodate health problems or disabilities.

(iv) **Religion or beliefs**: May be processed to accommodate religious or philosophical practices, such as dietary requirements related to religious or philosophical beliefs or religious holidays.

(v) **Sexual preference** (including Personal Information relating to partners of Individuals): May be processed to provide benefits to partners of Individuals.

(vi) **Biometric information** (e.g., fingerprints): May be processed for the protection of JPMC, Customers, and Employee assets, site access and for security reasons;

2. General Purposes for Processing Special Categories of Information

In addition to the specific purposes listed above, all categories of Special Categories of Information may be Processed under one (or more) of the following circumstances:

(i) as required or allowed for the performance of a task carried out to comply with a legal obligation to which JPMC is subject;

(ii) as required by or allowed under applicable local law or a collective agreement (with respect to Special Categories of Information about Employees);

(iii) for dispute resolution

(iv) for fraud prevention;

(v) to protect a vital interest of an individual, but only where it is impossible to obtain the individual's consent first;

(vi) to the extent necessary to comply with an obligation of public international law (e.g., a treaty); or

(vii) if the Special Categories of Information have been posted or otherwise shared at the individual's own initiative on JPMC social media or has manifestly been made public by the individual.

(viii) for Secondary Purposes in accordance with Article 2.2.

C. Consultation with Privacy Lead

Where there is a question whether a certain Processing of Personal Information can be based on a Business Purpose listed above, Staff should consult the appropriate Privacy Lead before the Processing takes place.

ANNEX 3 — SERVICES

Overview of JPMC Business

JPMC's activities are organized, for management reporting purposes, into four major reportable lines of business, as well as Corporate Functions (such as audit, HR) supporting the lines of business. JPMC's consumer business is provided by the Consumer & Community Banking ("CCB"), with the wholesale lines of business being Corporate & Investment Bank ("CIB"), Commercial Banking ("CB"), and Asset & Wealth Management ("AWM") (which has two separate sub lines of business called Asset Management and Wealth Management).

JPMC has a relatively small retail banking presence in the Covered Jurisdictions, which is confined to wealth management, plus some discrete retail and wealth products. In other words, the direct collection of personal information from individuals in the Covered Jurisdictions is relatively limited, and most of JPMC's business is 'B2B' i.e. transacted with other corporate entities and businesses. In some of those B2B areas, for instance custodian or registrar services also acts as a Data Processor to those businesses, processing their customers' information in areas such as custody and funds services.

To best serve its business, JPMC has a significant number of centralised data processing centres and centralised service centres within individual lines of business, or by way of the Global Service Centres and Corporate Functions also across lines of business. The four lines of business also provide services to each other.

Consumer and Community Bank (CCB) business and data processing:

CCB offers services to consumers and businesses through bank branches, ATMs, online, mobile and telephone banking. CCB is organized into Consumer & Business Banking (including Consumer Banking/Chase Wealth Management and Business Banking), Mortgage Banking (including Mortgage Production, Mortgage Servicing and Real Estate Portfolios) and Card, Commerce Solutions & Auto. Consumer & Business Banking offers deposit and investment products and services to consumers, and lending, deposit, and cash management and payment solutions to small businesses. Mortgage Banking includes mortgage origination and servicing activities, as well as portfolios consisting of residential mortgages and home equity loans. Card, Commerce Solutions & Auto issues credit cards to consumers and small businesses, offers payment processing services to merchants, originates and services auto loans and leases, and services student loans.

CCB has its head office in U.S. but there is a cards business based in Ireland (Dublin) which is a merchant cards' acquirer run out of Chase Paymentech Europe Limited. There is also a data centre in Ireland which supports the CCB business in the EU and elsewhere. The CCB data centres in the US provide technology support for the business in the EEA and elsewhere.

Commercial Bank (CB) business and data processing:

CB delivers extensive industry knowledge, local expertise and dedicated service to U.S. and U.S. multinational clients, including corporations, municipalities, financial institutions and non-profit entities. In addition, CB provides financing to real estate investors and owners. Partnering with JPMC's other businesses, CB provides comprehensive financial solutions, including lending, treasury services, investment banking and asset management to meet its clients' domestic and international financial needs.

Almost all of CB's business is conducted in the United States, and international clients are, with very few exceptions, overseas subsidiaries of U.S. parented private companies. Within the EEA, the CB hub is the UK and CB has additional physical presences in Germany, The Netherlands, and Luxembourg.

Corporate Investment Bank (CIB) business and data processing:

The CIB consists of Banking and Markets & Investor Services, offers a broad suite of investment banking, market-making, prime brokerage, and treasury and securities products and services to a global client base of corporations, investors, financial institutions, government and municipal entities.

The CIB predominantly conducts business to business (B2B) activities, which consequently involve only limited PI. However, the CIB does process individuals' data particularly in the following areas: provision of fund registration services through our Transfer Agency service and when processing payment transactions. Additionally, to fulfil regulatory obligations the CIB would also ask for proof of identity information when on boarding clients, identification of related parties and conducting anti-money laundering checks.

Asset & Wealth Management (AWM) business and data processing:

AWM is a global leader in investment and wealth management. AWM clients include institutions, high net-worth individuals and retail investors in many major markets throughout the world. AM offers investment management products and services to institutional and individual investors across the world. The vast majority of AM clients utilise products falling into at least one of three general categories: investment advisory services through segregated mandates, alternative funds, and registered funds. For Wealth Management clients, AWM also provides retirement products and services, brokerage and banking services including trusts and estates, loans, mortgages and deposits.

Corporate Functions operation and data processing:

The Corporate segment consists of Treasury and Chief Investment Office and Other Corporate, which includes corporate staff units and expense that is centrally managed. The major Other Corporate units include Real Estate, Enterprise Technology, Legal, Compliance, Finance, Human Resources, Internal Audit, Risk Management, Oversight & Control, Corporate Responsibility and various Other Corporate groups. These groups are organised to cover the business globally within teams often based in multiple jurisdictions. To best support the business a number of centres of excellence have been developed based in various global locations. Data centres are located to facilitate the data processing efficiency, security, and business continuity needs of the business.

Global Service Centres: The four main Global Service Centres supporting the lines of business globally are based in Argentina, India, Philippines and Poland.

Human Resources operations and data processing:

HR consists of teams that include business partners and specialty functions which include, but are not limited to:

- Staffing – Manage the recruiting of highly talented and qualified candidates to support the resource needs of the businesses and support functions globally.
- Talent & Development – Create the leadership framework that includes the assessment, development and succession of JPMC's top executives. Establish core management training curriculum considering all levels of management globally.
- Compensation & Benefits – Design and manage compensation plans and programs, including equity and other long-term incentive plans. Develop and deliver competitive health and retirement benefits to meet different employee needs, goals and lifestyles.
- Employee Relations – Oversee the investigation and resolution of workplace issues globally, including the design and administration of HR policies, with a focus on fair and equitable processes.
- Diversity – Partner with senior management to drive policies and practices that support a diverse workforce and an inclusive environment for JPMC employees that embraces varied backgrounds, cultures, work styles and lifestyles.
- Operations – Provide self and assisted service channels for employees, managers, and the HR function for services such as, but not limited to employee data and records management, payroll,

timekeeping, employee query handling, onboarding and off-boarding operations, benefits administration, and relocation services.

The main data and service centres are in: UK, U.S.and India. HR supports JPMC through a combination of global systems and local systems.

ANNEX 4 — PRIVACY GOVERNANCE

Chief Privacy Officer

1. JPMorgan Chase & Co. has appointed a Chief Privacy Officer who also serves as the Data Protection Officer under EEA Data Protection Law, unless another person is appointed as a Data Protection Officer. The Chief Privacy Officer is responsible for the following responsibilities, which the Chief Privacy Officer may perform directly or delegate to personnel in the Privacy Office as appropriate:

   (i) Supervising compliance with this Privacy Code;

   (ii) Establishing and maintaining a global network of Privacy Leads sufficient to direct compliance with this Privacy Code;

   (iii) Advising on the information management processes, systems and tools to implement the privacy compliance framework as established by the Privacy Council;

   (iv) Maintaining an updated list of the Group Companies and records of updates to the Privacy Code;

   (v) Providing periodic privacy reports to Global Operating Committee on privacy protection risks and compliance issues as described in Article 12.3;

   (vi) Coordinating, in conjunction with the Privacy Leads and/or the appropriate compliance officers, official investigations or inquiries into the Processing of Personal Information by a public authority;

   (vii) Advising in respect of conflicts between this Privacy Code and applicable law, as described in Article 15;

   (viii) Approving transfers as described in Article 9;

   (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 Information is implemented as described in Article 11.4; and

   (x) Deciding on complaints as described in Annex 5.

Privacy Council

2. The Chief Privacy Officer is a member of the Privacy Council. The Privacy Council shall create and maintain a privacy compliance framework for:

   (i) Maintaining, updating and publishing of this Privacy Code and related sub-policies;

   (ii) Developing, reviewing and updating JPMC's privacy procedures, system information, DPIAs and, training and awareness programs (as required by Article 11);

   (iii) Overseeing the documentation notification and reporting of Information Security Breaches;

   (iv) Ensuring the internal audit systems to monitor, audit and report compliance with this Privacy Code and ensure that JPMC's internal audit team can verify and certify such compliance in line with its annual audit process;

   (v) Overseeing the collection, investigation and resolution of

privacy inquiries, concerns and complaints; and

(vi) Determining and updating appropriate sanctions for violations of this Privacy Code (e.g., disciplinary standards) in cooperation with other relevant internal functions, such as HR and Legal.

Privacy Office

3. The Chief Privacy Officer has established and shall maintain JPMC's Privacy Office, consisting of a global network of Privacy Leads, sufficient to direct compliance with this Privacy Code within their respective regions and organizations.

The Privacy Office shall perform at least the following tasks:

(i) Regularly advise the global JPMC organization and other relevant internal functions (e.g., marketing, HR, development) on privacy risks and compliance issues;

(ii) Implementing the privacy compliance framework (as developed by the Privacy Office in accordance with this Privacy Code);

(iii) Being available for requests for privacy approvals or advice;

(iv) Handling privacy-related requests and complaints;

(v) Owning and authorizing all appropriate privacy procedures in their respective regions and organizations;

(vi) Cooperating with the Chief Privacy Officer, other Privacy Leads and other relevant functions.

Responsible Executive

4. The Responsible Executive is accountable for his or her business organization's compliance with this Privacy Code, including:

(i) Ensuring availability of adequate resources and budget to implement the privacy compliance framework established by the Privacy Council;

(ii) Ensuring continued privacy compliance of his/her business organization during and following any restructuring, outsourcing, mergers and acquisitions and divestitures;

(iii) Ensuring that privacy requirements are taken into account whenever new technology is implemented in his or her business organization;

(iv) Ensuring implementation of the management processes, systems and tools to implement the privacy compliance framework established by the Privacy Council in his or her business organization;

(v) Ensuring and monitoring ongoing compliance of third parties with the requirements of this Privacy Code in cases where Personal Information is transferred by JPMC to a Third Party (including entering into a written contract with such Third Party and obtaining a sign off of such contract from the legal department);

(vi) Ensuring that relevant individuals in his or her business organization follow the prescribed privacy training courses;

(vii) Ensuring that stored Personal Information be deleted or

destroyed, de-identified or transferred as provided in this Privacy Code;

(viii) Maintaining (or ensuring access to) an inventory of the system information about the structure and functioning of all systems that Process Personal Information as provided in this Privacy Code;

(ix) Informing the Chief Privacy Officer of any new legal requirement that may interfere with JPMC's ability to comply with this Privacy Code; and

(x) Consulting with the Chief Privacy Officer in all cases where there is a conflict between applicable local law and this Privacy Code as described in Article 15 and determining how to comply with this Privacy Code where there is such a conflict.

Privacy Lead with a Statutory Position

5. Where a Privacy Lead holds his or her position pursuant to law, he or she shall carry out his or her job responsibilities to the extent they do not conflict with his or her statutory position.

ANNEX 5 — COMPLAINTS PROCEDURE

Complaints

1. Individuals may file a written complaint (including by email) in respect of any claim they have under Article 13 in accordance with the complaints procedure set forth in this Annex as well as any complaints procedure as set out in other policies or contracts. Individuals also may file a complaint or claim with the authorities or the courts in accordance with Article 13.2.

The complaint shall be forwarded to the appropriate Privacy Lead. The appropriate Privacy Lead shall:

(i) notify the Chief Privacy Officer;

(ii) analyze the complaint and, if needed, initiate an investigation; and

(iii) when necessary, advise the business on the appropriate measures for compliance, and monitor, through to completion, the steps designed to achieve compliance; and

(iv) maintain records of all complaints received, responses given, and remedial actions taken by JPMC.

The appropriate Privacy Lead may consult with any public authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Individual

2. JPMC will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Individual within one month of the date that the complaint was filed. The appropriate Privacy Lead shall inform the Individual in writing via the means that the Individual originally used to contact JPMC (e.g., via mail or email) either (i) of JPMC's position with regard to the complaint and any action JPMC has taken or will take in response or (ii) when he or she will be informed of JPMC's position, which shall be no later than two months after the communication was sent to the Individual in the event that JPMC cannot reasonably complete its investigation and response within one calendar month. The appropriate Privacy Lead shall send a copy of the complaint and his or her reply to the Chief Privacy Officer.

Complaint to Chief Privacy Officer

3. An Individual may file a complaint with the Chief Privacy Officer if the resolution of the complaint by the appropriate Privacy Lead is unsatisfactory to the Individual (e.g., the complaint is rejected or a response is not received within the applicable timeframes set out in Article 2 of this Annex 5); or

(i) the Individual has not received a response as required by Article 6.6;

(ii) the time period provided to the Individual pursuant to Article 6.6 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 or she will receive a response; or

(iii) in one of the events listed in Article 6.8.

The procedure described in sub 2 above also shall apply to complaints

filed with the Chief Privacy Officer.

If the response of the Chief Privacy Officer to the complaint is unsatisfactory to the Individual (e.g., the request is denied), the Individual can file a complaint or claim with the authorities or the courts in accordance with Article 13.