JPMorgan Chase & Co

GLOBAL PRIVACY CODE Summary

Binding Corporate Rules for the transfer of personal data

outside the EU and UK under Article 47 GDPR

1. What Are BCRs?

Binding Corporate Rules or "**BCRs**" are data protection policies that provide rules and safeguards for the international transfers of personal information within JPMC outside the EU. In order to facilitate international transfers of personal information, BCRs must be approved by the competent data protection authorities.

The BCRs of JP Morgan Chase & Co (**JPMC**, "**we**," or "**us**") were approved by the EU data protection authorities and are currently maintained by the data protection authority of Hessen (Germany). The JPMC BCRs have been found to provide adequate safeguards for the protection of personal information throughout our organization. This means that the JPMC BCRs can be used to facilitate transfers of personal information outside the EU in accordance with EU data protection law. In addition, JPMC has approved UK BCRs, which facilitates the use of the JPMC BCRs for transfers outside the UK in accordance with UK data protection law. Our UK BCRs are maintained with the UK's Information Commissioner ("ICO"). We refer to our BCRs as our **Global Privacy Code**.

You can read the JPMC BCRs, titled the "**Global Privacy Code**," in here. The Global Privacy Code is legally binding on, and enforced by, the JPMC group companies listed here.

Below, we summarize the data protection safeguards that are included in the Global Privacy Code, and your rights in this regard. If you have any questions, please contact the JPMC Privacy Office at emea.privacy.office@jpmchase.com.

2. When Does the Global Privacy Code Apply?

The Global Privacy Code applies to all personal information that is collected and used by a JPMC group company that is subject to EU or UK data protection law or that was subject to EU or UK data protection law prior to the transfer of such personal information outside the EU or UK. The Global Privacy Code only applies if the JPMC group company qualifies as a "controller," which means that it collects and uses personal information for its own purposes. If a JPMC group company collects and uses personal information on behalf of another company (*i.e.*, as a "processor"), the Global Privacy Code does not apply.

3. What Are the Data Protection Safeguards of the Global Privacy Code?

The Global Privacy Code provides extensive data protection safeguards that JPMC applies when the personal information is collected and used in the EU or UK and continues applying when the personal information is transferred abroad. The Global Privacy Code includes data protection safeguards on the following topics:

- **Lawfulness:** Collecting and using personal information only with a good reason (or "legal basis")—such as where we need to use personal information to conclude or perform a contract with you or where we are legally required to do so—or with your consent. We only use sensitive personal information where allowed by EU or UK data protection laws.
- **Purpose limitation:** Collecting and using personal information for the Business Purposes listed in Annex 2 to the Global Privacy Code, and for other purposes where we have a lawful basis for doing so. We only use information for another purpose (a "secondary purpose") than the one for which it was collected if the secondary purpose is closely linked to (or "compatible" with) the original purpose.
- **Accuracy:** Keeping personal information accurate and up to date.

- **Data minimization:** Using only the personal information that is reasonably adequate for, and relevant to, the purpose for which it is collected and is being used.
- **Data retention:** Storing personal information only for as long as necessary for the purpose for which it was collected or is being used.
- **Privacy by design and by default:** Implementing privacy-protective features in the design phase of technical and organizational processes.
- **Transparency:** Informing you about the way we collect and use your personal information, such as which information we collect, the purpose(s) for which we use it, and the organizations with whom we share it.
- **Individuals' rights:** Providing you with rights in relation to the collection and use of your personal information. You have the right to request access to, and correction, deletion, or restriction of, your personal information, and you have the right to object to certain uses of your personal information. You also have the right to data portability and the right to be notified regarding rectification, erasure, or restriction of your personal information. You may exercise your individual rights by using the contact details found in our privacy notices or by contacting the JPMC Privacy Office.

- **Automated decisions:** Not making decisions that have a significant negative outcome on you based solely on automated processing, unless we are legally required to do so, it is necessary to enter into or perform a contract with you, or you have given your explicit consent.
- **Data transfers:** Ensuring that your personal information is adequately protected by us and also when it is shared with service providers or other third parties. We ensure appropriate safeguards and protections are in place, including by conducting transfer impact assessments when transferring personal information to countries that have not been recognized as providing an adequate level of data protection, and by implementing supplementary measures where necessary to ensure compliance with the Global Privacy Code.

- **Data security and confidentiality:** Implementing appropriate technical, physical, and organizational measures to protect your personal information from misuse, loss, and unauthorized access. We will document information security breaches and notify the relevant data protection authority and/or the affected individuals thereof where required. Such notifications may be delayed as instructed by law enforcement, where it determines that such notifications would impede a criminal investigation or cause damage to national security.
- **Foreign laws and government access requests:** Informing the competent data protection authority if we become aware that an applicable local law of a foreign country is likely to have a substantial adverse effect on the protection offered by the Global Privacy Code. If we receive a legally binding request for disclosure of personal information from a public authority of a foreign country, we will assess the legality of such request and challenge requests that we consider unlawful, including by seeking interim measures to suspend the effects of the request. We will notify the relevant data exporter and, where possible, the affected individual of such request. Where notification is prohibited, we will use our best efforts to obtain a waiver of such prohibition. We will provide only the minimum amount of personal information permissible when responding to such a request, and will not make transfers of personal information to any public authority that are massive, disproportionate, or indiscriminate.

4. Governance, Monitoring, and Audits

To support our Global Privacy Code, we have a privacy governance program and develop and implement policies and procedures. This also includes conducting a prior assessment of the privacy impact of certain uses of personal information, where such uses are likely to result in a high risk to the rights and freedoms of individuals, in particular, where new technologies are used.

We periodically monitor and audit our business processes and procedures that involve the use of personal information for compliance with this Global Privacy Code. We ensure that adequate steps are taken to address noncompliance with this Global Privacy Code. We will provide the competent data protection authority with information regarding the outcomes of audits related to compliance with this Global Privacy Code, upon request.

5. Your Rights Under the Global Privacy Code

You may file a written complaint in respect of any claim you have under the Global Privacy Code in accordance with the complaints procedure set forth in the relevant privacy policy or contract.

We will use reasonable efforts to resolve complaints without undue delay, so that a response is given to you within one month of the date that the complaint was filed. If you consider the response to be unsatisfactory, you may file a complaint with the Data Protection Officer via emea.privacy.office@jpmchase.com.
In addition to making a complaint, you can enforce any claim as a result of a breach of the data protection safeguards set out in Section 3 above as a third-party beneficiary, including the right to obtain compensation for material and immaterial damages suffered as a result of a violation of the Global Privacy Code. Where you demonstrate that you have suffered damage and establish facts which show it is plausible that the damage has occurred because of a violation of the Global Privacy Code, it will be for the relevant JPMC entity to prove that the violation is not attributable to it. You also have the right to lodge a complaint with a data protection authority, in particular in the UK or EU Member State of your habitual residence, place of work, or place of the alleged infringement, and to bring a claim before the competent courts. These rights are not dependent on you having used the complaints procedure described above. We accept responsibility for breaches of the Global Privacy Code by our entities located outside the EU and UK.

Depending on your circumstances and location, you can enforce the data protection safeguards by submitting a complaint or claim with:

- **J.P. Morgan SE** in Germany, if the complaint or claim relates to processing of personal information subject to transfer requirements under EU laws and relating to JPMC's banking activities carried out by a branch or operating subsidiary of **JPMorgan Chase Bank, National Association** ("JPMCNA"); or

- **J.P. Morgan Asset Management (Europe) S.à.r.l.** in Luxembourg, if the complaint or claim relates to processing of personal information subject to transfer requirements under EU laws and relates to other activities than JPMC's banking activities, carried out by a Group Company that is not a branch or operating subsidiary of JPMCNA.

- **J.P. Morgan Chase, N.A., London Branch** in the UK, if the complaint or claim relates to processing of personal information subject to transfer requirements under UK laws and relating to JPMC's banking activities carried out by a branch or operating subsidiary of JPMCNA; or

- **J.P. Morgan Asset Management (UK) Limited** in the UK, if the complaint or claim relates to processing of personal information subject to transfer requirements under UK laws and relates to other activities than JPMC's banking activities, carried out by a Group Company that is not a branch or operating subsidiary of JPMCNA.

The rights that you have under the Global Privacy Code are supplementary rights only; they do not deprive you of any other rights or remedies that you may otherwise have by law.

6. Questions

If you have any questions about the Global Privacy Code or the protection of your personal information by JPMC in general, please contact us at emea.privacy.office@jpmchase.com.