CBR Business Risk and Compliance

Managing Personal Data Responsibly

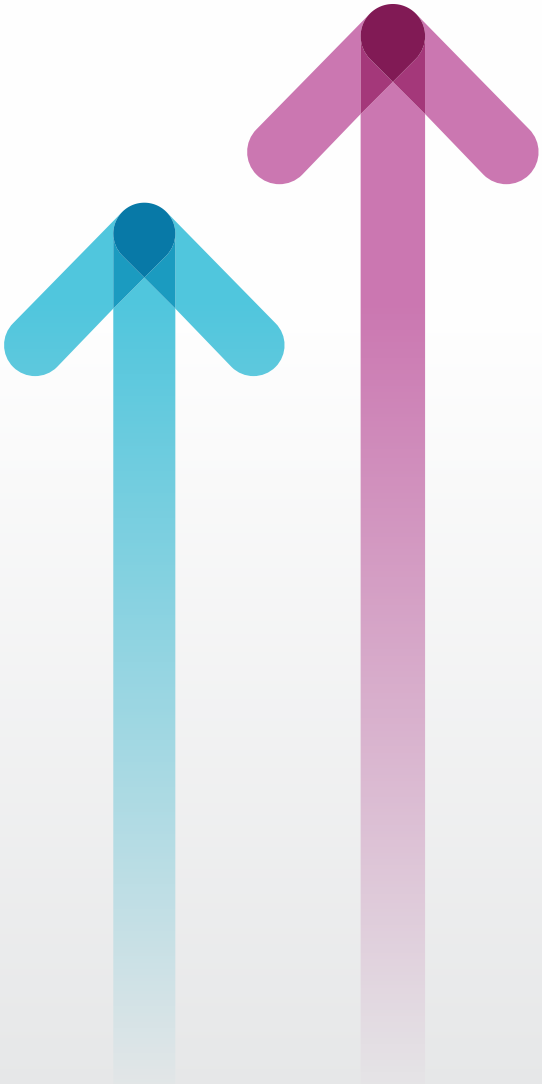
IFC Data Privacy Office

IFC International Finance Corporation
WORLD BANK GROUP

Creating Markets, Creating Opportunities

CBR Business Risk and Compliance

This booklet is intended to provide a summary of IFC's privacy framework. Neither IFC nor the World Bank make any representation, warranty or undertaking, express or implied, in respect of this booklet or any information contained herein; guarantee the completeness of the content of this booklet, or any conclusions or judgments described herein; or accept responsibility or liability for any omissions in the content of this booklet or for any reliance thereon. The contents of this work are intended for general informational purposes only and are not intended to constitute legal, securities, or investment advice, an opinion regarding the appropriateness of any investment, or a solicitation of any type. This booklet does not in any way constitute or imply a waiver, termination or modification by IFC of any privilege, immunity or exemption of IFC granted in its Articles of Agreement, international conventions, or applicable law.



Managing Personal Data Responsibly

The International Finance Corporation (IFC) — a member of the World Bank Group (WBG)[1] — is the largest global development institution focused exclusively on the private sector in emerging markets. Working with more than 2,000 partners worldwide, IFC provides and mobilizes capital, offers advisory services to companies and member states and harnesses global experience and innovative thinking to help clients overcome financial, operational and development challenges.

To do so, IFC utilizes innovative products and services and cutting-edge financial technologies. Underlying it all is data, which, when paired with technology, has expanded the frontiers of development. ***"Personal data," or information about individual people***, in particular, provides IFC with more comprehensive information to inform policy and investment decisions. This, in turn, allows IFC to maximize finance for development by understanding the needs of the individuals and communities impacted by its projects.

In this increasingly data-driven world, and with greater public focus on the use (and misuse) of data, responsibly managing personal data is key to IFC sustaining its reputation as a trusted partner and force for public good. Doing so demands a strong, modernized personal data management regime.

1. The World Bank Group (WBG) comprises five institutions: the International Bank for Reconstruction and Development (IBRD), the International Development Association (IDA, together with IBRD, the World Bank), the International Finance Corporation (IFC), the Multilateral Investment Guarantee Agency (MIGA), and the International Centre for Settlement of Investment Disputes (ICSID).

The ***IFC Data Privacy Office (DPO)*** is focused on the appropriate use and governance of personal data. At its core, this means meeting the ***reasonable expectations*** of our staff, clients and partners, as well as the communities impacted by IFC projects, regarding IFC's use of personal data.

Privacy Around the World

While views around privacy vary across cultures, ***over 130 countries from all regions*** of the world have put in place some form of legislation regarding privacy and data protection — a number that continues to increase. Requirements can differ widely from jurisdiction to jurisdiction, but at their core most reflect ***a set of foundational, high-level principles*** that are consistent across the globe.

Organizations that embrace these foundational principles are more likely to align with ***existing and evolving expectations*** around acceptable use of personal data. These organizations are better positioned to take advantage of technological advancements allowing ever more sophisticated uses of data, while effectively navigating the growing public attention and concern around personal data use.

The goal of the IFC Data Privacy Office is, above all, ***to help IFC responsibly manage the personal data it collects in its business activities and to meet the reasonable expectations of our clients and partners and the communities they serve***.

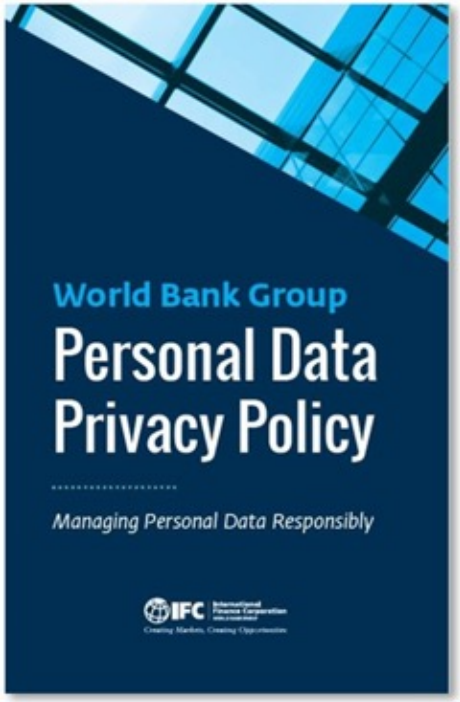
The World Bank Group Personal Data Privacy Policy

At the heart of IFC's data privacy program is a set of foundational principles shared by all WBG institutions and enshrined in the World Bank Group Personal Data Privacy Policy (the Privacy Policy).

The seven principles of the Privacy Policy were distilled from common core principles found in a range of international standards and instruments, including the ***Organisation for Economic Co-Operation (OECD) Privacy Framework***, ***Convention 108*** (Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Council of Europe Treaty Series 108) and the ***Asia-Pacific Economic Cooperation (APEC) Privacy Framework***.

The Privacy Policy was presented to, and approved by, the IFC Board of Directors and the Boards of the other WBG institutions in May of 2018.

After an implementation period, these principles became applicable to all WBG operations in February of 2021.



The Privacy Policy Principles

The seven principles of the Privacy Policy are summarized below:

1 *Legitimate, Fair and Transparent Processing*

Processing of personal data should be for a ***legitimate purpose***, and processing should be fair and transparent to the individual concerned (often called the data subject).

2 *Purpose Limitation and Data Minimization*

Personal data should be collected for one purpose and ***may not be used for another purpose***, except in accordance with the Privacy Policy; only the personal data needed to accomplish that purpose should be collected.

3 *Data Accuracy*

Personal data should be collected, recorded, and maintained as ***accurately*** as possible.

4 *Storage Limitation*

Personal data should be retained and disposed of according to ***applicable records retention and disposition schedules***.

5 *Security*

WBG institutions should use reasonable technical and organizational measures to ***avoid*** accidental destruction, loss, alteration, ***unauthorized disclosure*** of or access to personal data.

6 *Transfers of Personal Data*

Personal data should only be transferred to third parties for legitimate purposes and ***with appropriate regard for protection*** of the personal data transferred.

7 *Accountability and Review*

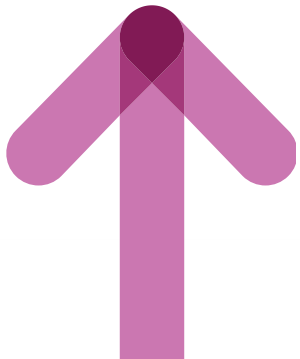
WBG institutions are required to adopt documentation, processes, and procedures appropriate to ***implement and oversee compliance*** with the Privacy Policy.

IFC Approach to Personal Data Protection

The IFC privacy program consists of three main pillars built upon the foundational principles set out in the Privacy Policy.

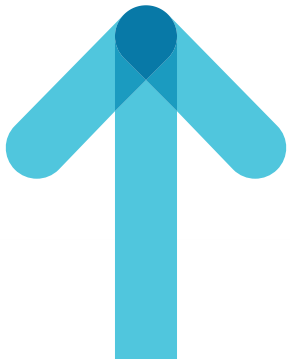
Policies and Procedures

Development of policies and procedures that operationalize the Privacy Policy for the day-to-day activities of IFC staff.



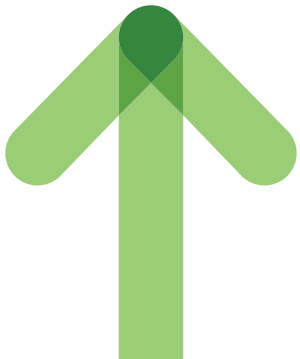
Technology

Implementation of appropriate technical safeguards against unauthorized processing and accidental loss, destruction or damage; privacy by design.



Awareness and Training

Educating IFC staff on key privacy concepts and training them on their responsibilities under the Privacy Policy and IFC's privacy-related policies and procedures.



IFC Data Privacy Office (DPO)

At IFC, Management has delegated functional authority for IFC's privacy program to the DPO. The DPO is established as a function of the Business Risk and Compliance Department within the Legal and Compliance Risk Vice Presidency. It is staffed by a cross-functional team and led by the Chief Data Privacy Officer.

The DPO develops, establishes and maintains the privacy posture and risk appetite for IFC regarding the processing of personal data, consistent with the Privacy Policy.

As part of its role the DPO:

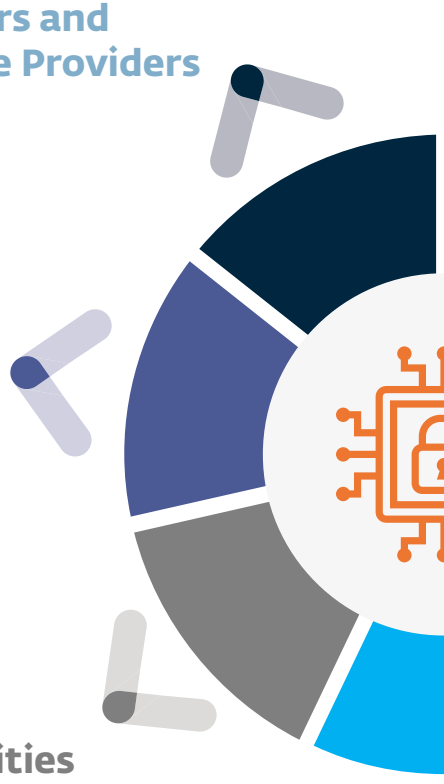
1. Serves as the central coordinating body and focal point for IFC privacy-related issues.
2. Advises IFC Staff on appropriate use of personal data and the identification, assessment and mitigation of risks associated with the processing of personal data.
3. Develops IFC's privacy-related policies and procedures and trains IFC staff on their use.
4. Responds to requests from individuals seeking information regarding their personal data processed or held by IFC or, where appropriate, seeking redress in accordance with the Privacy Policy.
5. Collaborates with other WBG institutions' data privacy offices as well as other IFC departments on privacy-related matters.
6. Provides privacy business requirements related to information technology services to the WBG Information and Technology Solutions Department.

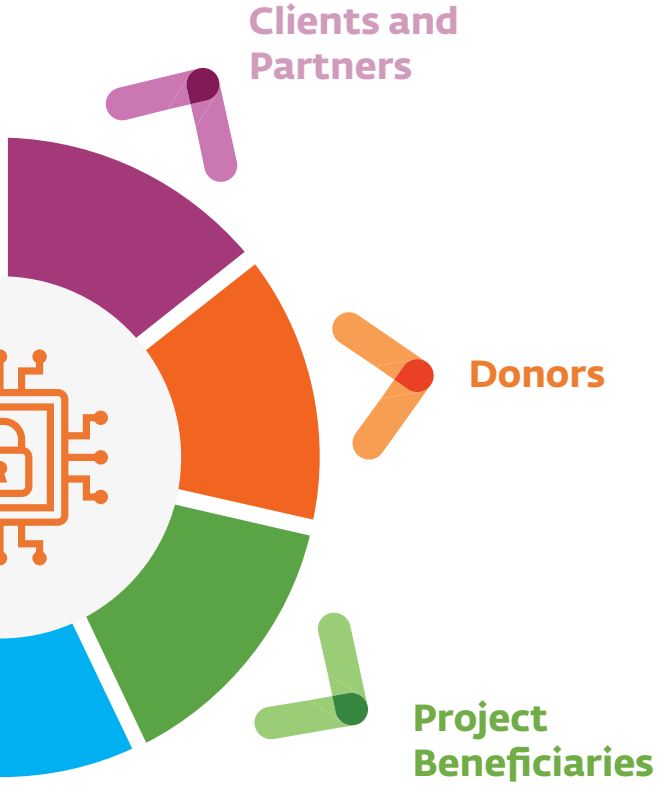
To support the work of the DPO, each IFC department designates a **Privacy Coordinator**. Privacy Coordinators serve as their department's liaison to the DPO, receive enhanced training and help support greater collaboration between the DPO and IFC staff in the field.

What Personal Data does IFC Process?

IFC processes personal data in a variety of contexts:

- Personal data processed in the course of providing IFC's products and services (e.g., when conducting due diligence on individuals associated with clients and partners)
- Visitors to IFC's websites
- Subscribers of IFC Newsletters or Publications
- Registered attendees of IFC Events
- Personal data processed in the context of HR processes (e.g., recruitment)
- Personal data processed in the context of procurement (e.g., when conducting background checks related to potential vendors)





For what reasons can IFC collect and process personal data under the Privacy Policy?

The Privacy Policy states IFC may only process personal data for "legitimate purposes". A legitimate purpose is defined as any purpose:

- Carried out with the consent of the individual whose personal data is being processed.
- In the vital or best interest of a relevant individual.
- Necessary for performance of a contract or other binding obligation or undertaking.
- Consistent with, or reasonably necessary to enable IFC to carry out its mission, mandate or purpose.

More information, including detailed privacy notices covering processing in the context of IFC's Products & Services, Events and Websites is available at ifc.org/privacy.

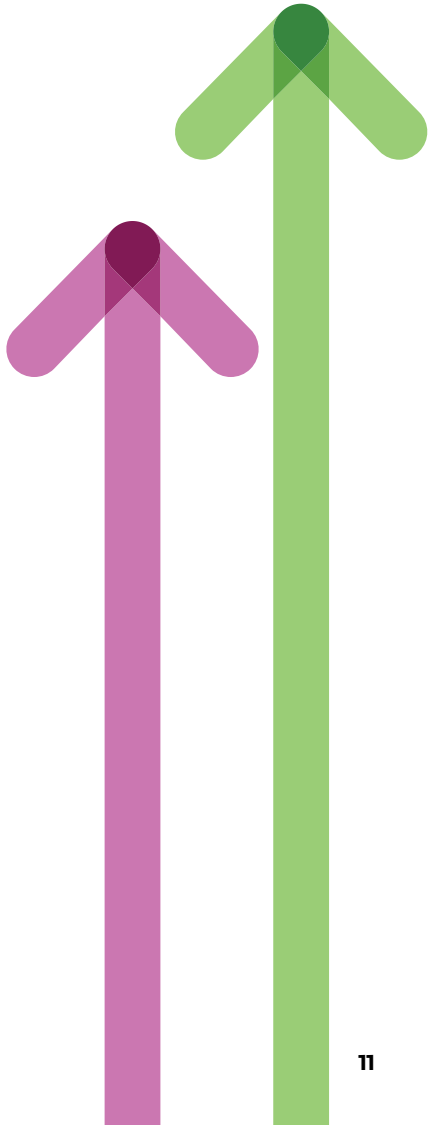
IFC deploys ***a number of tools and strategies*** to responsibly manage personal data and mitigate privacy risk, depending on the circumstances. Collectively these tools and strategies make-up ***a robust privacy risk management framework*** designed to give effect to the principles of the Privacy Policy.

Managing and Mitigating Privacy Risk

The process of managing personal data in IFC operations is governed by the IFC privacy risk management framework. This framework is designed to identify potential privacy risk early – ***before any personal data has been processed*** – to provide maximum opportunity to put in place mitigants consistent with the Privacy Policy.

The IFC privacy risk management framework consists of:

- Mandatory privacy risk assessments, designed to be completed by IFC staff early in the project cycle and evaluated centrally by the DPO.
- Comprehensive privacy clauses in relevant IFC legal templates, clearly setting forth IFC's privacy expectations.
- An integrated case-management system for timely advice to IFC staff requesting guidance.
- Tailored privacy management arrangements for IFC activities that consistently involve the processing of personal data.
- A continuous staff training and awareness program.



Examples

EXAMPLE 1:

An IFC Advisory team has been engaged by a client to provide HR management advice and will need to view information related to the ***client's employees***.

IFC STAFF MITIGATE PRIVACY RISK BY:

- ***Limiting*** the personal data collected by IFC to what is necessary to complete the project. If possible, collecting only aggregated or anonymized data.
- If personal data is necessary, ***minimizing the amount and type of personal data*** collected.
- Including ***appropriate privacy clauses*** in the relevant legal agreement.
- Observing ***confidentiality and security obligations arising from contractual provisions*** and IFC policies and procedures.

Information on Contractual Language

Whenever IFC is receiving personal data from a third-party (e.g., a client or partner) it must often rely on such third-party to obtain the appropriate permissions and consents necessary to share the personal data with IFC. Typically, IFC receives these assurances ***through a written legal agreement that includes the third-party's obligations with respect to the personal data provided to IFC***. Data privacy provisions to this effect are now standard in IFC's relevant legal templates.

EXAMPLE 2:

An IFC Upstream team is conducting a ***survey*** of micro, small and medium enterprises (MSMEs) to gather information about the local business climate.

IFC STAFF MITIGATE PRIVACY RISK BY:

- Designing the survey to collect the ***least amount of personal data*** necessary to provide IFC with the information it needs.
- Including ***privacy notice language*** at the beginning of the survey and, as appropriate, collecting acknowledgments from participants that they have read and understood how their personal data will be used.
- Observing the ***limitations*** set forth in the privacy notice language.
- Observing the ***confidentiality and security obligations*** arising from IFC policies and procedures.

Data Minimization in IFC Operations

Data minimization is another core principle of the Privacy Policy and one of the key mitigants of privacy risk. Under this principle, IFC ***minimizes the amount and type of personal data collected*** to what is needed to achieve the purpose of the processing. For example, if the only personal data IFC needs for this project is the names and email addresses of MSME contacts, then only this personal data — and nothing additional — should be collected in the survey. If personal data is not necessary, then none should be collected.

EXAMPLE 3:

An IFC Knowledge Management team is setting up a new ***externally-facing website*** that will collect personal data from website visitors.

IFC STAFF MITIGATE PRIVACY RISK BY:

- Following ***privacy-by-design principles*** and developing the website to collect only the amount and type of personal data necessary for the website's purpose.
- Drafting a ***privacy notice*** tailored to the website, stating what personal data will be collected, how IFC will use it and with whom IFC will share the data.
- Linking the privacy notice on ***all pages*** of the website.
- Observing the ***limitations*** set forth in the privacy notice.
- Observing the ***confidentiality and security obligations*** arising from IFC's digital governance and IT policies and procedures.

Information on Privacy Notices

Fair and transparent processing is a core requirement of the first principle of the Privacy Policy. One of the key ways to achieve this is by providing an appropriate ***privacy notice*** to individuals whose personal data will be processed. A privacy notice is a document that provides individuals with ***details regarding how their personal data will be used*** (e.g., what personal data will be collected, how it will be used, who will have access to it, how long it will be kept, etc.). When IFC is collecting personal data directly from individuals, IFC staff are responsible for preparing and providing a privacy notice. When IFC receives the personal data from a third-party, it must often rely on that party to prepare and provide an appropriate privacy notice (an issue typically addressed in the legal agreement between IFC and the relevant third-party).

EXAMPLE 4:

IFC shares personal data with a ***partner*** as part of a joint development project.

IFC STAFF MITIGATE PRIVACY RISK BY:

- Confirming the sharing of personal data is ***reasonably necessary*** to complete the joint development project.
- Confirming the sharing is ***consistent with the specific purpose*** for which the personal data was collected.
- Ensuring any ***necessary consents*** to sharing have been obtained.
- Including appropriate ***safeguards and use limitations*** in the legal agreement with the partner.

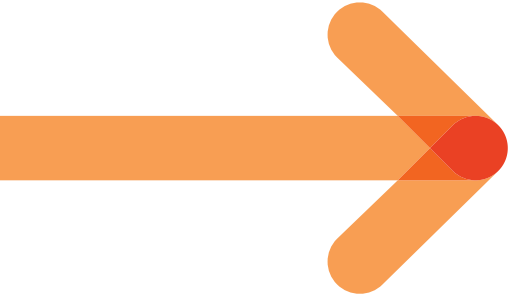
Sharing Data for Development

Data, including personal data, is at the heart of development. Sharing of data between development partners is also a common and necessary practice. When the purpose of a project requires the sharing of personal data, ***extra precautions*** are put in place to confirm that the sharing is consistent with the requirements of the Privacy Policy. For example, in the project above, IFC would typically include language in the ***legal agreement*** requiring ***appropriate security*** for the data and placing ***specific limitations*** on use, sharing and retention of the shared personal data to address the requirements of the transfer principle of the Privacy Policy.

Privacy Across the WBG

With a single WBG Privacy Policy establishing a common set of principles, the institutions of the WBG share a ***consistent and collaborative approach to privacy***. Staff working on data privacy issues at different institutions meet regularly to coordinate, discuss matters of mutual interest and reinforce a culture of privacy awareness across the WBG.

However, due to their unique mandates, each WBG institution has operationalized the Privacy Policy in a manner tailored to its specific business needs. The result is a ***shared WBG approach*** to privacy that is implemented on an ***institution-by-institution*** basis.



For more information on the privacy programs of IFC's sister WBG organizations please visit:

World Bank: worldbank.org/en/about/legal/privacy-notice

MIGA: miga.org/privacy

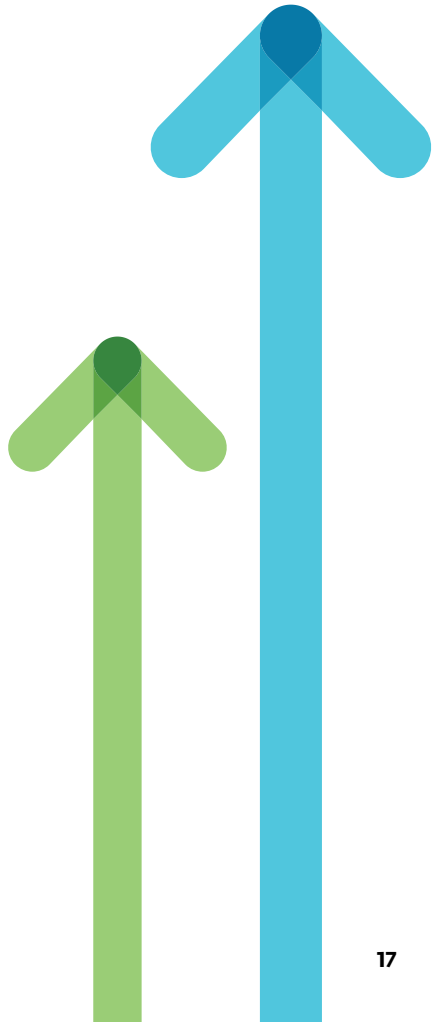
ICSID: icsid.worldbank.org/about/content/privacy-policy

Review and Redress Mechanism

As part of its data privacy framework, IFC has established a ***mechanism for individuals to request information regarding their personal data*** processed or held by IFC and, when appropriate, to seek redress.

Individuals can submit a ***request*** with respect to their personal data held by IFC, in accordance with principle seven of the Privacy Policy, by following the steps outlined in IFC's Personal Data Review & Redress Mechanism Statement (available at ifc.org/privacy).

IFC's review and redress mechanism is applicable only to personal data held by IFC. Requests related to personal data held by another WBG institution must be submitted in accordance with that institution's mechanism. Information about how to submit requests to the World Bank, MIGA and ICSID can be found at each institution's website (see links on previous page).



For more information on IFC's commitment to manage personal data responsibly please visit ifc.org/privacy

Questions regarding IFC's privacy practices can be directed to ifcdataprivacy@ifc.org

IFC International Finance Corporation
WORLD BANK GROUP
Creating Markets, Creating Opportunities

2121 Pennsylvania Avenue, NW
Washington, DC 20433 USA