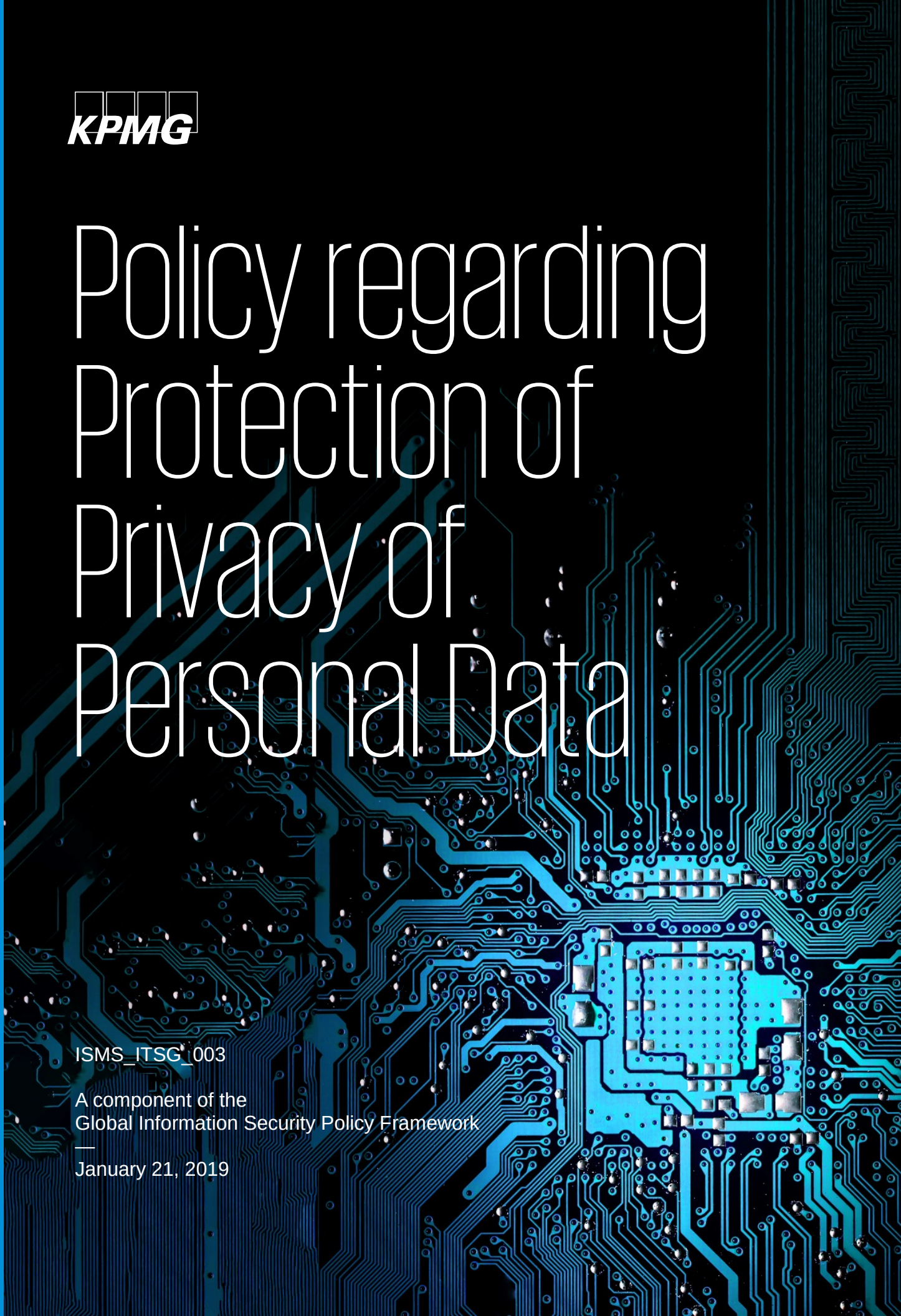

Policy regarding Protection of Privacy of Personal Data

ISMS_ITSG_003

A component of the
Global Information Security Policy Framework

—

January 21, 2019

Document ownership, validity, review and approval

Document ownership, validity	
Ownership	
The nominated owner of this document is the Global Chief Privacy Officer.	
Validity	
This document is valid as of	2011.06
Retirement date	N/A

Document revision history (last revision)			
Version	Author	Revision	Date
Final 1.0	IRMO	Reviewed and approved with no substantive changes being made	2015.03
Final 2.0	IRMO	Reviewed and approved with changes	2018.01
Final 2.1	Martin Hilger	Template updated, no content changes	2018.06.12
Final 2.2	Martin Hilger	Content reviewed by IRMO, no content changes	2019.01.21

Document reviews (last, next reviews)			
Reviewer	Review cycle	Last review	Next review
Parsons, Gordon – IRSO Kraml, Willi – GISO Giller, Irina – LLP Parsons, Nick – ELLP Kistler, Kami	V1.0	2013.08	N/A
IRMO	V2.0	2018.01	2019.01
Lynn Marvin (IRMO)	V2.1 (yearly - FY18)	2018.09.18	2019.01
Lynn Marvin (IRMO)	V2.2 (yearly - FY19)	2019.01.21	2020.01.21

Document approvals (last approvals)		
Name	Comment	Last approval
Global Information Technology Steering Group (GITSG)		2011.06
IRWG	V1.0	2013.08
Global Chief Privacy Officer	V2.0 (FY18)	2018.01
Global Chief Privacy Officer	V2.2 (FY19)	2019.01

Document applicability and limitations

This document applies to KPMG International, KPMG member firms and other KPMG entities worldwide.

KPMG member firms operate globally in many different jurisdictions. In case of conflict, local laws and other mandatory regulations always override KPMG policies, requirements and standards.

Users of this document should ensure they are consulting the extant version of this material.

Contents

1 Document Control

IPG policies, standards and guidelines are maintained under the governance, processes and procedures described in the **Information Protection Policy Framework**.

Online versions of these materials are maintained in an automation tool and made accessible for authorized users via the IPG intranet portal. Offline versions of the materials contain the same content as the portal and are provided via Live Documents/PDF files generated by the automation tool.

The only official copy of this PDF document is located **here**.

1.1 Document control procedure

The document control procedure for this document is described in ISMS_ITSG_009.

2 Introduction

2.1 Scope

This Policy has been adopted in order to assist in establishing and maintaining an adequate level of personal data privacy in the collecting, processing, disclosing and cross-border transfer of personal data including that relating to current, past and prospective KPMG personnel, clients, suppliers, contractors and business associates of the KPMG Firms.

For the Scope of Policy please see Section 3.3.

2.2 Audience

Core audiences for this document:

— KPMG Member Firms and KPMG Personnel.

3 Policy regarding Protection of Privacy of Personal Data

3.1 Preface

KPMG International, a cooperative formed under the laws of Switzerland and headquartered in the Netherlands, has adopted this policy about the privacy of Personal Data (the "Policy"). The Policy has been adopted in order to assist in establishing and maintaining an adequate level of Personal Data privacy in the collecting, processing, disclosing and cross-border transfer of Personal Data including that relating to current, past and prospective KPMG Personnel, clients, suppliers, contractors and business associates of the KPMG Firms. The Policy was last reviewed in January 2019 to reflect the KPMG Network's proposed adoption of Binding Corporate Rules.

3.2 Definitions

- **"Controlled Party (ies)"** means any legal entity which is wholly or dominantly owned and controlled by a KPMG Firm.
- **"Individual"** means any identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity.
- **"Inter-Firm Agreement"** means the agreement entered into between the KPMG Firms setting out the terms on which international transfers of Personal Data are to be carried out within the network of KPMG Firms.
- **"KPMG International"** means KPMG International a cooperative organized and existing under the laws of Switzerland and headquartered in the Netherlands.
- **"KPMG Firms"** means (i) KPMG International (and any other 'KPMG Network Entity' as such term is defined in the Inter Firm Agreement) and (ii) any member firm or sublicensee of KPMG International (including the Controlled Parties) which is duly authorized to use the "KPMG" name and/or trade and/or service marks and "KPMG Firm" shall mean each of them.
- **"KPMG Personnel"** means all partners, directors, officers, employees, individual contractors and other personnel of a KPMG Firm.
- **"Local Personal Information"** and **"Local Personal Data"** both mean Personal Data in respect of which a KPMG Firm can demonstrate that it has both not been: (i) processed outside of the jurisdiction in which the KPMG Firm is established; or (ii) disclosed to another KPMG Firm.

— **"Personal Information"** and **"Personal Data"** both mean any information that relates to an identifiable living Individual (not companies or other legal persons).

— **"processing"** of Personal Data shall mean any operation or set of operations that is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, restriction, erasure or destruction.

— **"Sensitive Personal Data"** means Personal Data: (i) revealing information as to an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, offences, criminal convictions, criminal history, trade union membership, genetic data, biometric data, health, sex life or sexual orientation; or (ii) which does not fall into any of the categories in (i), but which is (a) regulated under national privacy law in the jurisdiction from which it was exported in the same manner as those types of Personal Data and (b) the relevant KPMG Firm has informed KPMG International that the Personal Data should be treated as sensitive personal data.

3.3 Scope of Policy

This Policy only applies to Personal Data which is processed by or on behalf of a KPMG Firm and:

1 is or was processed at any time by or on behalf of KPMG Firms in a jurisdiction which is either: (a) in the EU or EEA; or (b) not in the EU or EEA, but is a jurisdiction which imposes similar restrictions on the use or extra-territorial transfer of Personal Data; and

2 is not Local Personal Data.

This Policy does not apply to Local Personal Data. Decisions and compliance in relation to Local Personal Data is the preserve of the relevant KPMG Firm.

This Policy should not conflict with applicable national and/or regional laws in the jurisdictions in which KPMG Firms operate and the Policy shall be so construed wherever possible. In the event of any conflict between this Policy and any applicable national and/or regional laws, the provisions of the relevant law shall govern. In this event, the relevant KPMG Firm shall immediately notify Global Quality Risk Management and the office of KPMG International's General Counsel.

3.4 KPMG's Ten Principles for Handling Personal Data as a Controller

In handling Personal Data as a controller, KPMG Firms and KPMG Personnel will abide by the following ten key principles:

1 Transparency:
KPMG Firms will provide individuals with information about how we process their Personal Information to the extent necessary to ensure that processing is fair.

2 Purpose limitation:

KPMG Firms will only process Personal Information for the purposes (i) set out in any notice made available to the relevant individuals which are relevant to KPMG; (ii) as required by law or (iii) where consented to by the relevant individuals.

3 Data quality and proportionality:

Personal Data should be kept accurate and where necessary, up to date. The Personal Information KPMG Firms hold must be adequate, relevant and not excessive for the purposes for which they are transferred between the KPMG Firms and should only be retained for as long as necessary for the purposes of the relevant processing.

4 Security and confidentiality:

Reasonable precautions must be taken to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. These precautions should include technical, physical and organizational security measures, such as measures to prevent unauthorized access, that are commensurate with the sensitivity of the information and the level of risk associated with the processing of the Personal Data. From time to time, the applicable measures may be documented more fully in IT and risk management policies adopted by the KPMG Firms.

Where necessary or appropriate, KPMG Firms must consider implementing additional measures for particular types of Personal Data that may need to be handled with additional care, so as to respect local customs, laws or regulations. This may include Sensitive Personal Data.

Where a KPMG Firm processes Personal Information on behalf of another KPMG Firm, it will only act under the first firm's instructions.

5 Access, rectification, deletion and objection:

Individuals should have access to their Personal Data that is held by KPMG Firms, where those requests are reasonable and permitted by law or regulation. KPMG Firms agree to rectify, amend, or delete Personal Information upon request where it is inaccurate or where it is being used contrary to these key principles.

An individual should be able to object to the processing of the Personal Data relating to them if there are compelling legitimate grounds relating to their particular situation, to the extent required by relevant laws.

6 Sensitive Data:

Where KPMG Firms process Sensitive Personal Data, they will take such additional measures (e.g., relating to security) as are necessary to protect such Sensitive Personal Data in accordance with applicable law.

7 Data used for marketing purposes:

Where KPMG Firms process Personal Information for the purposes of direct marketing, those KPMG Firms will have effective procedures allowing individuals at any time to "opt-out" from having their Personal Information used for such purposes.

8 **Automated Processing:**
Where KPMG Firms process Personal Information on a purely automated basis that has a significant impact on an individual, those KPMG Firms shall give the individual the opportunity to discuss the output of such processing before making those decisions (save to the extent otherwise permitted under applicable law).

9 **Data minimization:**
Where KPMG Firms retain an individual's personal information, those KPMG Firms will do so in a form identifying or rendering an individual identifiable only for so long as it serves the purpose(s) for which it was initially collected or subsequently authorised except to the extent permitted by applicable law; and

10 **Information transfer and compliance:**
Within the global network of KPMG Firms, Personal Data may be transferred outside the country in which it was collected, including countries outside of the European Economic Area, for legitimate business activities in accordance with applicable law. In addition, in accordance with applicable law, the KPMG Firms may store Personal Data in facilities operated by other KPMG Firms and/or third parties on behalf of the KPMG Firms outside the country in which the data was collected.

Nevertheless, Personal Data must not be transferred to another country unless the transferor has assurance that an adequate level of protection is in place in relation to that Personal Data as required under applicable law. In the case of each KPMG Firm, an adequate level of protection is created by the Inter-Firm Agreement which each KPMG Firm shall abide by.

KPMG Firms will ensure that where personal information is transferred to third parties outside of the KPMG network for processing (for example to KPMG's service providers to support KPMG's business), that this is only done where the personal information is adequately protected. KPMG Firms will achieve this by entering into written agreements with third parties which impose obligations that reflect the requirements of this policy.

3.5 Enforcement

Any breach of this Policy may lead to the suspension, and ultimately termination of the offender's authority to access such Personal Data. Any usage of the Personal Data other than in the manner set out in this Policy may further subject the offender to discipline by the relevant KPMG Firm in which he or she is directly engaged up to and including termination of employment, as well as possible civil and/or criminal penalties.

3.6 Acting as a Processor

Where KPMG Firms act in a capacity as a processor of Personal Data on behalf of clients, they should act in accordance with the instructions of the controller of such Personal Data. If this is not possible for any reason (for example due to a conflict with current or future legislation), the relevant KPMG Firm will promptly inform the client (directly or via another KPMG Firm) of its inability to comply with their instructions. When a KPMG Firm ceases to act on behalf of a client, it will (at the client's option) return, destroy or continue to properly protect all personal data it had received from that client.

Where a KPMG Firm acts as such a processor, it also has a duty to help the client comply with the law (subject to the client meeting the KPMG Firm's related costs and expenses), for example (i) by informing the client about the processing activities that KPMG carry out so that they may inform the relevant individuals; (ii) at the clients request putting in place reasonable measures to have that data updated, corrected, anonymized or deleted (subject to certain limited exceptions), and inform other firms within the KPMG network where such changes are made; and (iii) sending to the client any requests they receive from individuals for access to their personal information that the KPMG Firm holds, so that the client may respond to those individuals.

Where acting as such a processor of Personal Data, KPMG Firms will in any event treat such Personal Data in accordance with the above paragraphs relating to Security and confidentiality and Information transfer and compliance, only transfer Personal Information where the client has agreed to such a transfer (which it may do in advance under the terms of engagement with the relevant KPMG Firm) and inform the client if there is serious breach of security in relation to personal information so that they can inform the individuals concerned, where necessary.

A KPMG Firm will be "controller" where they determine the purposes and means by which Personal Data is used. KPMG Firms are likely to be controllers in relation to all employee data. KPMG Firms will be "processors" where they process Personal Data on behalf of a "controller" who instructs them how they can use the data. KPMG Firms will often be "processors" on those client engagements where they are only entitled to use the Personal Data disclosed to them to perform the relevant engagement.

3.7 International Databases

For legitimate business and professional reasons, KPMG International has created, will continue to create, and will maintain, systems and applications that contain Personal Data about KPMG Personnel (and, where applicable, their immediate family members) and clients, suppliers, contractors and business associates. These systems and applications are part of the shared electronic communications, knowledge management, and information technology environments of the KPMG Firms and are used to share this Personal Data between KPMG Firms to the extent permitted by law and applicable professional standards. A list of these systems and applications is maintained by KPMG International and is available to KPMG Firms.

3.8 Complaints, Questions and Additional Information.

To express a concern, raise a question, make a complaint, or to obtain additional information about the processing of Personal Data by the global network of KPMG Firms, the concerned individual should contact the Privacy Liaison for the relevant KPMG Firm in the first instance.

Contact us

Ian Dennis
Global Chief Privacy Officer
T +1 617 331 1682
E iandennis@kpmg.com

www.kpmg.com