



Verizon Enterprise Solutions

Binding Corporate Rules Processor Policy

Contents

INTRODUCTION TO THIS POLICY	3
PART I: BACKGROUND AND ACTIONS	4
PART II: PROCESSOR OBLIGATIONS	6
PART III: APPENDICES	13

INTRODUCTION TO THIS POLICY

This Binding Corporate Rules Processor Policy ("**Policy**") establishes the approach taken by Verizon Enterprise Solutions (also referred to as Verizon Wireline and Verizon Business) ("**Verizon**") to the protection and management of personal information¹ globally by Verizon group members ("**Group Members**") when processing² that information on behalf of a third party or another Group Member and where such personal information originates from Europe.

This Policy applies to all personal information originating from Europe and collected and processed as part of the regular business activities of Verizon in the course of providing services to a third party or another Group Member (equally referred to as the "customer" in this Policy), and Group Members and their employees must comply with and respect this Policy when collecting and processing personal information in their capacity as service providers.

This Policy does not replace any specific data protection requirements that might apply to a business area or function.

This Policy and a list of Group Members is published on the website accessible at www.verizon.com.

¹ Personal information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in EU Directive 95/46/EC.

² For the purposes of this Policy reference to the 'processing' of personal information is as defined in EU Directive 95/46/EC, and references to 'collection' 'use' and 'transfer' are all elements of the definition of processing.

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

European data protection law gives people the right to control how their personal information is used. Under data protection law, when an organisation collects, uses or transfers personal information for its own purposes, that organisation is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the legal requirements.

When, on the other hand, an organisation processes information on behalf of a third party or a different member of its corporate group that organisation is deemed to be a *processor* of the information and the third party will be primarily responsible for meeting the legal requirements. So for example where we provide services as a global telecommunications provider we will be acting as a data processor in respect of the personal data of our customers.

HOW DOES DATA PROTECTION LAW AFFECT VERIZON INTERNATIONALLY?

Data protection law does not allow the transfer of personal information to countries outside Europe³ that do not ensure an adequate level of data protection. Some of the countries in which Verizon operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

When Verizon acts as a processor, Verizon's European customers retain the responsibility to comply with European data protection law. When a Group Member acts as a processor in circumstances where the controller located in Europe is another Group Member, the Group Member acting as controller will retain the responsibility to comply with European data protection law.

In practical terms, this means that those acting as controllers must pass certain data protection obligations onto any processor which processes personal information outside Europe on behalf of those controllers in order to overcome the legal restrictions on international data transfers.

If Verizon fails to comply with the data protection obligations imposed on it by its customers, Verizon's customers may be in breach of applicable data protection law and Verizon may face a claim for breach of contract which may result in the payment of compensation or other judicial remedies. In such cases, if a customer demonstrates that it has suffered damage, and that it is likely that the damage occurred because of a breach of this Policy the obligation will be for Verizon UK Ltd to show that a Verizon entity outside Europe (or a third party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place

WHAT IS VERIZON DOING ABOUT IT?

The purpose of this Policy is to set out a framework to satisfy the standards contained in European data protection law and, as a result, provide an adequate level of protection for all personal information transferred to Group Members outside Europe either where the personal information is collected by a customer in Europe as a controller or where the personal information is collected by Verizon in Europe as a processor.

Although it will be for each of Verizon's customers to decide whether the commitments made by Verizon in this Policy provide adequate safeguards for the personal information transferred to Verizon under the

³ For the purpose of this Policy reference to Europe means the EEA **and** Switzerland.

terms of its contract with Verizon, Verizon will apply the Rules contained in this Policy whenever it acts as a processor. Where Verizon's customers rely upon this Policy as providing adequate safeguards, a copy of this Policy will be incorporated into the contract with that customer. If a customer of Verizon chooses not to rely upon this Policy, that customer will have the responsibility to put in place other adequate safeguards to protect the personal information.

Verizon will apply this Policy globally where Verizon processes personal information as a processor both manually and by automatic means and such personal information originates from Europe as identified in the contract with the customer.

This Policy applies to all Group Members and their employees worldwide and requires that Group Members who collect, use or transfer personal information to provide services to a third party as a processor or who provide a service to other Group Members in their capacity as a processor comply with the Rules set out in **Part II** of this Policy together with the policies and procedures set out in the appendices in **Part III** of this Policy.

For completeness, Group Members must comply with the Binding Corporate Rules Controller Policy when they collect use and transfer personal information as a controller. Some Group Members may act as both a controller and a processor and must therefore comply with this Policy and also the Binding Corporate Rules Controller Policy as appropriate.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you can contact Verizon's Director, Privacy Policy & Compliance International at the address below who will either deal with the matter or forward it to the appropriate person or department within Verizon.

Attention: Director, Privacy Policy & Compliance International

Email: emeadataprotection@intl.verizon.com

Telephone: + 44 (0)118 905 5000

Address: Director, Privacy Policy & Compliance International, Verizon, 3rd Floor, Spur D, Reading International Business Park, Basingstoke Road, Reading, RG2 6DA

The Director, Privacy Policy & Compliance International is responsible for ensuring that changes to this Policy are notified to the Group Members' customers and to individuals whose personal information is processed by Verizon in accordance with Appendix 7.

If you are unhappy about the way in which Verizon has used your personal information Verizon has a separate complaint handling procedure which is set out in Part III, Appendix 5.

PART II: PROCESSOR OBLIGATIONS

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles that Verizon must observe when Verizon collects and uses personal information as a processor.
- Section B deals with the practical commitments made by Verizon to the European data protection authorities when Verizon collects and uses personal information.
- Section C describes the third party beneficiary rights that Verizon has granted to individuals in its capacity as a processor under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – Verizon will ensure that compliance with this Policy will not conflict with data protection laws where they exist.

To the extent that any applicable data protection legislation requires a higher level of protection than is provided for in this Policy, Verizon acknowledges that it will take precedence over this Policy.

Rule 1B – Verizon will co-operate and assist a controller to comply with its obligations under data protection law in a reasonable time and to the extent reasonably possible.

Verizon will, within a reasonable time and to the extent reasonably possible and as may be required under contracts with its customers, assist customers on request to comply with their obligations as controllers under applicable data protection law. For example, Verizon will be transparent about sub-processor activities so that its customers may correctly inform data subjects.

RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – Verizon will assist a controller to comply with the requirement to explain to individuals at the time their personal information is collected how that information will be used.

Verizon's customers have a duty to explain to individuals, at the time their personal information is collected or shortly after, how that information will be used. Verizon will provide such assistance and information to its customers as may be required under the terms of its contract with its customers to comply with this requirement, for example, information about any sub-processors appointed by Verizon to process customer personal information on its behalf.

Rule 2B – Verizon will only process personal information on behalf of and in accordance with the instructions of the controller.

Verizon will only process personal information in compliance with the terms of the contract it has with its customers.

If, for any reason, Verizon is unable to comply with this Rule or its obligations under this Policy in respect of any contract it may have with a customer, Verizon will inform the customer promptly of this fact. Verizon's customer may then suspend the transfer of personal information to Verizon and/or terminate the contract, depending upon the terms of its contract with Verizon.

In such circumstances, Verizon will act in accordance with the instructions of its customer and return, destroy or store the personal information, including any copies of the personal information, in a secure manner or as otherwise required by its customer.

In the event that legislation prevents Verizon from returning the personal information to its customer or destroying it, Verizon will ensure that such information remains confidential and will not process the personal information otherwise than in accordance with the instructions of its customer.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3A – Verizon will assist controllers to keep the personal information accurate and up to date to the extent reasonably possible.

Verizon will comply with any instructions from its customers in order to assist them to comply with their obligation to keep personal information accurate and up to date.

When required to do so on instruction from its customers, Verizon will delete, anonymise, update or correct personal information. Where personal information cannot, for technical reasons, be deleted Verizon will advise its customers accordingly and take steps to put such personal information beyond use.

Verizon will notify other Group Members or any third party sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

In practice, when Verizon acts for a customer in its capacity as a cloud provider, Verizon does not have access to the personal information of its customers and so when acting in this capacity Verizon is unlikely to be required to delete, anonymise, update or correct such personal information.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – Verizon will assist controllers to comply with the rights of individuals.

Verizon will act in accordance with the instructions of its customers and undertake any reasonably necessary measures to enable its customers to comply with their duty to respect the rights of individuals. In particular, if any Group Member receives a subject access request, the Group Member will transfer such request promptly to the relevant customer and not respond to such a request unless authorised to do so. Verizon will follow the steps set out in section 6 of the Subject Access Request Procedure (see Appendix 1).

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – Verizon will always adhere to the security and organisational measures required by the applicable data protection law as specified in a contract with a controller.

European law expressly requires that where Verizon provides a service to a customer which involves the processing of personal information, the contract between Verizon and its customer imposes clear obligations dealing with the security of that information consistent with the law of the European country applicable to the customer to ensure that Verizon has in place proportionate technical and organisational security measures to safeguard the personal information.

Group Members will always adhere to the security and organisational measures specified in contracts with their customers.

Rule 5B – Verizon will always notify a controller of any security breach in particular in accordance with the law as it applies to Verizon as a telecommunications provider.

Group Members will notify a customer without undue delay of any security breach in relation to personal information processed on behalf of that customer in accordance with the law as it applies to Verizon as a telecommunications provider.

Verizon's obligations in its contracts with its customers are based on the requirements of European law as it relates to telecommunications operators. This requires telecommunications operators established in Europe to notify security breaches to data protection authorities and, under certain circumstances, the subscribers/individuals concerned or other providers of electronic communication services.

Verizon will comply with its internal breach notification procedures as amended and updated from time to time which seek to achieve a standardised consistent approach based on European law and which apply to all Group Members wherever they are established.

Rule 5C – Verizon will comply with the requirements of a controller regarding the appointment of any sub-processor.

Verizon will inform its customers where processing undertaken on its behalf will be conducted by a sub-processor and will comply with the particular requirements of a customer with regard to the appointment of sub-processors as set out under the terms of its contract with that customer. Verizon will ensure that up to date information regarding its appointment of sub-processors is available to those customers at all times so that their general consent is obtained before the data have been transferred to a new sub-processor. If, on reviewing this information, a customer objects to the appointment of a sub-processor to process personal information on its behalf, that customer will be entitled to take such steps as are consistent with the terms of its contract with Verizon and as referred to in Rule 2B of Part II of this Policy (i.e. Verizon's customer may then suspend the transfer of personal information to Verizon and/or terminate the contract, depending upon the terms of its contract with Verizon).

Rule 5D – Verizon will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms in its contracts with its customers and (ii) this Policy, and in particular that the sub-processor will adopt appropriate and equivalent security measures.

Group Members must only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by Verizon in this Policy. In particular, such sub-processors must be able to provide appropriate technical and organisational measures that will govern their use of the personal information to which they will have access in accordance with the terms of the Group Member's contract with its customer.

To comply with this Rule, where a sub-processor has access to personal information covered by this Policy, Verizon will take steps to ensure that it has in place proportionate technical and organisational security measures to safeguard the personal information and will impose strict contractual obligations in writing on the sub-processor which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Policy (and in particular Rules 5A and 5B above) and with the terms of the contract Verizon has with its customer in respect of the processing in question;
- that the sub-processor will act only on Verizon's instructions when using that information; and
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Verizon in this Policy and which, in particular, provide for adequate safeguards (as understood in European law) with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of personal information from a Group Member in Europe to a sub-processor established outside Europe.

SECTION B: PRACTICAL COMMITMENTS

RULE 6 – COMPLIANCE

Rule 6 – Verizon will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Verizon has appointed its Director, Privacy Policy & Compliance International as the person to oversee and ensure compliance with this Policy supported by legal and compliance officers at regional and country level who are responsible for overseeing and enabling compliance with this Policy on a day to day basis. A summary of the roles and responsibilities of Verizon's privacy team is set out in Appendix 2.

RULE 7 – TRAINING

Rule 7 – Verizon will provide appropriate training to employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to process personal information in accordance with the Privacy Training Requirements attached as Appendix 3.

RULE 8 – AUDIT

Rule 8 – Verizon will comply with the Audit Protocol set out in Appendix 4.

RULE 9 – COMPLAINTS

Rule 9 – Verizon will comply with the Complaint Handling Procedure set out in Appendix 5.

RULE 10 – CO-OPERATION WITH DPAs

Rule 10 – Verizon will comply with the Co-operation Procedure set out in Appendix 6.

RULE 11 – UPDATES TO THE POLICY

Rule 11 – Verizon will comply with the Updating Procedure set out in Appendix 7.

RULE 12 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 12A – Verizon will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Policy, Verizon will promptly inform (unless otherwise prohibited by law):

- **the controller, as provided for in Rule 2B;**
- **Verizon's Director, Privacy Policy & Compliance International; and**
- **the data protection authority competent for the controller**

Rule 12B – Verizon will ensure that where it receives a legally binding request for disclosure of personal information transferred outside Europe under this Policy, Verizon will, unless prohibited from doing so by a law enforcement authority:

- **promptly notify the controller; and**
- **put the request on hold and promptly notify the data protection authority competent for the controller and the Information Commissioner's Office.**

Where Verizon receives a legally binding request for disclosure of information transferred outside Europe under this Policy and is prohibited by a law enforcement authority from putting the request on hold and/ or from notifying the relevant data protection authorities, Verizon will:

- use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as it can and as soon as possible to the relevant data protection authorities; and,
- demonstrate to the relevant data protection authorities the steps it followed to deal with the request in accordance with this Policy.

Verizon will provide to the relevant data protection authorities on an annual basis general information about the nature and number of such requests that it receives and will ensure that any transfers that it makes to a public authority in the context of this Rule 12B are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Where personal information is transferred under this Policy and where: (i) the individual whose personal information is transferred is unable to bring a claim against the controller because the controller has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law, that individual will have the following third party beneficiary rights:

- (a) to seek enforcement of compliance with this Policy;
- (b) to make a complaint to a European data protection authority in the jurisdiction of the European Group Member acting as a processor, or where there is no such Group

Member, in the jurisdiction from which the personal information is transferred and/or to a Group Member in Europe;

- (c) to bring proceedings against Verizon UK Ltd in:
 - (i) the courts of the UK;
 - (ii) in the jurisdiction of the European Group Member from which the personal information was transferred; or
 - (iii) in the jurisdiction of the European Member State where the individual resides;
- (d) where appropriate, to receive compensation from Verizon UK Ltd for any damage suffered as a result of a breach of this Policy by:
 - (i) any non- European Group Member; or
 - (ii) by any third party data processor which is established outside the Europe and which is acting on behalf of Verizon

in accordance with the determination of the court or other competent authority;
- (e) to obtain a copy of this Policy and the Intra-group agreement.

In the event that an individual suffers damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Policy, the burden of proof to show that a Group Member or any third party sub-processor which is established outside Europe and which is acting on behalf of a Group Member is not responsible for the breach, or that no such breach took place, will rest with Verizon UK Ltd.

Verizon UK Ltd will ensure that any necessary action is taken to remedy any breach of this Policy by a Non-European Group Member or any sub-processor which is established outside Europe and which is processing personal information on behalf of a customer.

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions ("Verizon")

Subject Access Request Procedure

1. Introduction

- 1.1 When Verizon collects, uses or transfers personal information for Verizon's own purposes, Verizon is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the requirements of data protection law.
- 1.2 When Verizon acts as a controller, individuals whose personal information is collected and/or used in Europe¹ have the right to be informed by Verizon whether any personal information about them is being processed by Verizon. This is known as the right of subject access.
- 1.3 In addition, all individuals whose personal information is collected and/or used² in Europe by Verizon acting as controller, and transferred between Verizon group members ("**Group Members**") will also benefit from the right of subject access and such subject access requests will be dealt with in accordance with the terms of this Subject Access Request Procedure ("**Procedure**").
- 1.4 This Procedure explains how Verizon deals with a subject access request relating to personal information which falls into the categories in sections 1.2 and 1.3 above (referred to as "**valid request**" in this Procedure).
- 1.5 Where a subject access request is subject to European data protection law because it is made in respect of personal information collected and/or used in Europe, such a request will be dealt with by Verizon in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.

2. Individuals' rights

- 2.1 An individual making a valid request to Verizon when Verizon is a controller of the personal information requested is entitled to:

¹ In this Procedure Europe means the EEA plus Switzerland

² This will include any personal information originally collected outside Europe and sent to Group Members in Europe for processing.

- 2.1.1 Be informed whether Verizon holds and is processing personal information about that person;
- 2.1.2 Be given a description of the personal information (including the categories of personal information) , the purposes for which they are being held and processed and the recipients or classes of recipient to whom the information is, or may be, disclosed by Verizon; and
- 2.1.3 Communication in intelligible form of the personal information held by Verizon.
- 2.1.4 The request must be made in writing, which can include email, using the form provided in Appendix 1 if possible.³
- 2.2 Verizon must deal with a valid request within 40 calendar days of its receipt (or such shorter period as may be stipulated under local law) of receipt of that request.
- 2.3 When the individual making the valid request is not an employee of Verizon, Verizon is not obliged to comply with a subject access request unless Verizon is supplied with such information that it may reasonably require in order to confirm the identity of the individual making the request so that Verizon is able to refine its search criteria appropriately in order to locate the information which that person seeks.

3. Process

- 3.1 Receipt of a subject access request when Verizon is a controller of the personal information requested.
 - 3.1.1 If Verizon receives any request from an individual for their personal information, this must be passed to the Director, Privacy Policy & Compliance International immediately upon receipt indicating the date on which it was received together with any other information which may assist the Director, Privacy Policy & Compliance International to deal with the request.
 - 3.1.2 The request does not have to be official or mention data protection law to qualify as a subject access request.
- 3.2 Initial steps

³ Unless the local data protection law provides that an oral request may be made, in which case Verizon will document the request and provide a copy to the individual making the request before dealing with it.

- 3.2.1 The Director, Privacy Policy & Compliance International will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.
- 3.2.2 The Director, Privacy Policy & Compliance International will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

4. Exemptions to the right of subject access for requests made to Verizon as a controller

- 4.1 A valid request may be refused on the following grounds:
 - 4.1.1 Where the subject access request is made to a European Group Member and relates to the use or collection of personal information by that Group Member, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located; or
 - 4.1.2 Where the subject access request does not fall within section 4.1.1 because it is made to a non-European Group Member and the Director, Privacy Policy & Compliance International is unable to deal with the request :
 - (a) if, in the opinion of Verizon, : (i it is necessary to do so to safeguard national or public security, defence, the prevention, investigation, detection and prosecution of criminal offences; or (iii) for the protection of the data subject or of the rights and freedoms of others (which includes the essential business interests of Verizon); or
 - (b) if the personal information is held by Verizon in non-automated form and is not or will not become part of a filing system; or
 - (c) where the personal information does not originate from Europe and the provision of the personal information requires Verizon to use disproportionate effort.

5. Verizon's search and the response

- 5.1 The Director, Privacy Policy & Compliance International will arrange a search of all relevant electronic and paper filing systems.

- 5.2 The Director, Privacy Policy & Compliance International may refer any complex cases to the Executive Director, Legal & Regulatory Affairs Europe for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.
- 5.3 The information requested will be collated by the Director, Privacy Policy & Compliance International into a readily understandable format (internal codes or identification numbers used at Verizon that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Director, Privacy Policy & Compliance International which includes information required to be provided in response to a subject access request.
- 5.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in section 2.1 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.
- 6. **Subject access requests made to Verizon where Verizon is a processor of the personal information requested**
 - 6.1 When Verizon processes information on behalf of a customer (for example, to provide a service) Verizon is deemed to be a *processor* of the information and the client will be primarily responsible for meeting the legal requirements as a controller. This means that when Verizon acts as a processor, Verizon's customer retain the responsibility to comply with applicable data protection law.
 - 6.2 Certain data protection obligations are passed to Verizon in the contracts Verizon has with its customer and Verizon must act in accordance with the instructions of its customer and undertake any reasonably necessary measures to enable its customer to comply with their duty to respect the rights of individuals. This means that if any Group Member receives a subject access request in its capacity as a processor for a customer, that Group Member must transfer such request promptly to the relevant customer and not respond to the request unless authorized by the customer to do so.

7. Requests for erasure, amendment or cessation of processing of personal information

- 7.1 If a request is received for the erasure, amendment, or cessation of processing of an individual's personal information where Verizon is the controller for that personal information, such a request must be considered and dealt with as appropriate by the Director, Privacy Policy & Compliance International.
- 7.2 If a request is received advising of a change in an individual's personal information where Verizon is the controller for that personal information, such information must be rectified or updated accordingly if Verizon is satisfied that there is a legitimate basis for doing so.
- 7.3 When Verizon deletes, anonymises, updates, or corrects personal information, either in its capacity as controller or on instruction of a customer when it is acting as a processor, Verizon will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.
- 7.4 If the request made to Verizon as a controller is to cease processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by Verizon, or on the basis of other compelling legitimate grounds, the matter will be referred to the Director, Privacy Policy & Compliance International to assess. Where the processing undertaken by Verizon is required by law, the request will not be regarded as valid.
- 7.5 All queries relating to this Procedure are to be addressed to the Director, Privacy Policy & Compliance International.

Appendix 1: Subject access request form

This form is to be used when you are wishing to exercise your right of access to information held about you by Verizon. This process will provide you with personal data held about you in manual and electronic form. Information relating to third parties may be withheld from you and/or other information exempt under applicable law(s).

Please complete your details below and sign where indicated. Send the completed form, proof of identity (when required), and other relevant information to:

Director, Privacy Policy & Compliance International (Third Floor Spur D), Verizon, Reading International Business Park, Basingstoke Road, Reading, RG2 6DA

Agents of the Data Subject: Please note that you must provide your own contact details and you **must** provide proof of your entitlement to act on the Data Subject's behalf.

Please complete as much of the following information as you can:	
Full name of Data Subject:	
	, (title) (last) (first)
Present Address:	
Town	
County	
Postcode	
Other contact details:	
Telephone	
E Mail	
Mobile:	
Previous Address (if different in past 3 years)	
Town	
County	
Postcode	
Date of Birth (dd/mm/yy)	

Current/ last post held in Verizon (if applicable)	
Department	
Office location	
Your PeopleSoft/employee no.	

Details regarding what information you are looking for	To help us to meet your request as quickly as possible, please provide as much detail regarding the information you seek.
Hard copy files (specify department & location if known)	
Search criteria (i.e. name, key word, date),	
Connection to file (employee/ customer/supplier)	
Electronic data specify system if known	
Search Criteria (system name, identifier no.,if known)	
Connection to file (employee/ customer)	
Any other filing system	
Search criteria	

Any other information to assist us in meeting your request:	
--	--

Signed: _____

Date: _____

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions (Verizon)

Compliance Structure

1. Overview

- 1.1 Verizon's Organisational Privacy Structure (the "**OPS**") is a global network of privacy professionals. The structure of the OPS is shown on the attached diagram (Annex 1).
- 1.2 The OPS is split into two operational limbs: the US Privacy Team and Legal & Regulatory Affairs. The latter covers all regions where Verizon has a presence other than the US, namely, Europe, Latin America, Asia Pacific and Canada. The responsibilities of each team in the OPS and the reporting channels are clearly identified.
- 1.3 **Verizon's US Privacy Team** is led by the Vice President & Deputy General Counsel – Chief Privacy Officer (the "**CPO**"). The CPO reports to the Senior Vice President Public Policy who has responsibility for Verizon's global public policy, federal legislative affairs, federal regulatory affairs, strategic alliances, national security, privacy, and corporate citizenship.
- 1.4 **Legal & Regulatory Affairs** has two separate branches for Asia Pac and Europe. These are led, respectively, by the General Counsel – Asia Pac and by the Executive Director, Legal & Regulatory Affairs Europe. Both report to the Senior Vice President & General Counsel.
- 1.5 Both the Senior Vice President & General Counsel and the Senior Vice President Public Policy report directly to the Executive Vice President & General Counsel.
- 1.6 The OPS allows Verizon to deal with region specific issues arising due to the global nature, and scope, of Verizon's operations. Although the OPS is organised along regional lines, Verizon privacy personnel work together on projects to ensure a consistent approach where necessary.

2. Legal & Regulatory Affairs: Verizon's privacy structure outside the US

- 2.1 Legal & Regulatory Affairs encompasses the privacy functions of Verizon's operations in Europe, Asia Pacific, Canada and Latin America. In these territories Verizon personnel manage privacy issues based on their geographical region and in-country expertise.

Europe

2.2 The Director, Privacy Policy & Compliance International

2.2.1 The Director, Privacy Policy & Compliance International, based in Verizon's European HQ in the UK is responsible for all aspects of EU privacy compliance and processing pursuant to the EU Data Protection Directive 95/46/EC and applicable laws throughout Verizon's Group Members.

2.2.2 More specifically, the Director, Privacy Policy & Compliance International's responsibilities include:

- Ensuring Verizon's compliance with Verizon's Binding Corporate Rules controller and processor policies;
- In cases where the Internal Audit Department identifies areas of non-compliance with Verizon's Binding Corporate Rules controller and processor policies, ensuring that these are corrected within a reasonable timescale.
- Reviewing new products and services relating to privacy matters to ensure compliance with EU privacy law(s);
- Maintaining and updating Verizon's EU specific privacy policies and privacy-related instructions;
- Counselling business units on internal and external privacy principles and requirements;
- Ensuring Verizon's compliance with EU privacy laws, regulations, principles and policies;
- Responding to regulatory bodies and industry organisations regarding opinions/proposals/drafts on proposed changes to EU privacy legislation and policy;
- Working with Verizon Security on security issues which relate to customer or employee privacy;
- Providing privacy face to face and net-conference training where employees (in teams such as Human Resources; Sales; Customer Services; and Billing) are required to have a heightened awareness of EU privacy issues;
- Providing privacy training and updates to employees on existing and new privacy law and policies, including the Binding Corporate Rules controller and processor policies;
- Assisting the commercial legal team in contract negotiations and ensuring that Verizon's contracts reflect the requirements of EU privacy law;
- Ensuring compliance with all in-country elements of EU privacy law including, where necessary, that data protection registrations and notifications are

complete and permits for the international transfer of personal data are obtained.

2.3 The Director, Privacy Policy & Compliance International reports to the Executive Director, Legal & Regulatory Affairs Europe.

2.3.1 EU Regulatory Officers

In addition to the Director, Privacy Policy & Compliance International, Verizon has a team of in-country EU Regulatory Officers who are responsible for data protection compliance in all European countries where Verizon operates. Regulatory Officers assist local employees with specific in-country privacy issues and are a conduit for communication between the Director, Privacy Policy & Compliance International and local data protection authorities where required.

2.4 Latin America, Canada & Asia Pacific

Verizon has a team of privacy professionals in these regions who normally deal with specific regional issues and whose roles and responsibilities are similar to that of the Director, Privacy Policy & Compliance International, for which the General Counsel for the Asia Pacific region has overall responsibility.

3. US Privacy Team: Verizon's privacy structure in the US

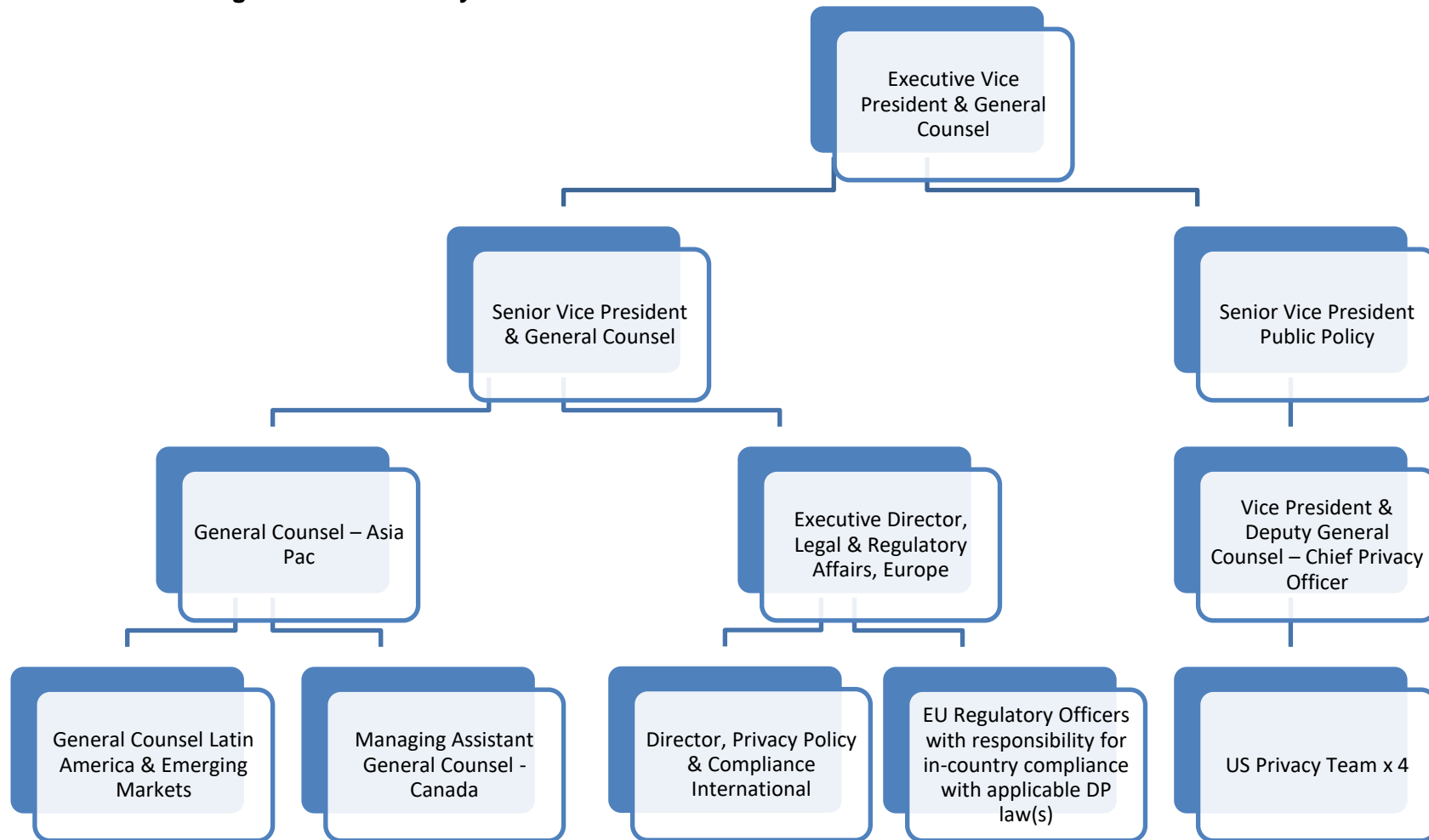
3.1 The Verizon US Privacy Team serves as a centralised privacy and compliance function within the US.

3.2 The Verizon US Privacy Team is responsible for:

- Reviewing new products and services relating to US privacy matters;
- Maintaining and updating Verizon's US facing privacy policies and privacy-related instructions to ensure compliance with US law;
- Counselling business units on internal and external privacy principles and requirements;
- Ensuring Verizon's compliance with US privacy laws, regulations, principles and policies;
- Responding to federal and state legislative and regulatory proposals that address the issue of privacy;
- Working with Verizon Security on security issues which relate to US customer or employee privacy; and
- Providing privacy training and updates to employees on existing and new privacy law and policies.

- 3.3 In addition to the functions described above, the CPO sits on the company's Compliance Council and Network and Technology Security Council. The CPO also reports to the Audit Committee of the Board of Directors and regularly meets with Verizon's Internal Audit team.

Annex 1 – Verizon Organisational Privacy Structure



Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions ("Verizon")

Privacy Training Requirements

1. Background

- 1.1 The Controller and Processor Data Protection Binding Corporate Rules of Verizon (the "**Policies**") provide a framework for the transfer of personal information between Verizon group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how Verizon trains its staff (the "**employees**") on the requirements of the Policies.
- 1.2 Verizon's Corporate Compliance Department has overall responsibility for compliance training within Verizon, including the delivery and tracking of Verizon's privacy training programs. Training on the Policies is overseen by the Director, Privacy Policy & Compliance International, the Chief Privacy Officer and in-region privacy professionals around the Globe.
- 1.3 All Verizon employees receive periodic training on privacy and data protection (the "**General Privacy training**") and on Verizon's Code of Conduct. Training on other specific privacy related matters such as Records Management, HIPAA Privacy and Security, or country-specific Data Protection, is also provided on a need to know basis.
- 1.4 Employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information receive additional, tailored training on the Policies (the "**BCR Policies training**") and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.
- 1.5 The General Privacy training and the BCR Policies training together are referred to in this document as the "**Privacy and compliance training program**".

2. Overview of training at Verizon

- 2.1 All Verizon employees are required to participate in the General Privacy training program once every two years. The program is called "*Keys to Safeguarding Privacy and Protecting Data*". This program is alternated with biennial training on Verizon's Code of Conduct, which also covers privacy obligations.

2.2 The General Privacy training covers a range of subjects, including data privacy, data protection breaches, and Verizon's Privacy and Information Security policies and procedures.

2.3 In addition to the yearly training described in section 2.1 and 2.2, Verizon also provides specific training on the Policies as described in section 4 below.

3. Aims of the Privacy and compliance training program at Verizon

3.1 The aim of Verizon's **Privacy and compliance training program** is to help create and maintain an environment in which:

3.1.1 employees have an understanding of the basic principles of data privacy, confidentiality, and information security;

3.1.2 employees understand Verizon's Privacy and Information Security policies and procedures; and

3.1.3 employees in positions having permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information, receive appropriate training, as described in section 4, to enable them to process personal information in accordance with the Policies.

3.2 General data protection and privacy training for new joining employees

3.2.1 New employees must complete the General Privacy training, the BCR Policies training (if required) and training on Verizon's Code of Conduct shortly after joining Verizon. The Code of Conduct requires employees to follow Verizon's Privacy and Information Security policies and procedures.

3.3 General data protection and privacy training for all employees

3.3.1 Employees worldwide receive the General Privacy training. This training covers basic data privacy rights and principles and data security in line with the requirements of the Policies. It is designed to be both informative and user-friendly, generating interest in the topic. Completion of the course is monitored and enforced by Verizon's Corporate Compliance Department, which drives 100% completion by

all required employees annually and is accountable to the Audit Committee of the Board of Directors.

3.3.2 All employees also benefit from:

- (a) Code of Conduct training, which provides a detailed review of Verizon's commitment to ethical behaviour, including specific discussion of key ethics and compliance risks; and
- (b) ad-hoc communications consisting of emails, awareness messaging placed on Verizon's intranet pages and information security posters displayed in offices which convey the importance of information security and data protection issues relevant to Verizon, including for example, social networking, remote working, engaging data processors and the protection of confidential information

4. BCR Policies training

4.1 Verizon's training on the Policies will cover the following main areas and employees receive training appropriate to their roles and responsibilities within Verizon:

4.1.1 Background and rationale:

- (a) What is data protection law?
- (b) How data protection law will affect Verizon internationally
- (c) The scope of the Policies
- (d) Terminology and concepts

4.1.2 The Policies:

- (a) An explanation of the Policies
- (b) Practical examples
- (c) The rights that the Policies gives to individuals

- (d) The data protection and privacy implications arising from the processing of personal information on behalf of clients

4.1.3 Where relevant to an employee's role, training will cover the following procedures under the Policies:

- (a) Subject Access Request Procedure
- (b) Audit Protocol
- (c) Updating Procedure
- (d) Cooperation Procedure
- (e) Complaint Handling Procedure

5. Further information

Any queries about training under the Policies should be addressed to the Corporate Compliance Department which can be contacted at: Verizon.Compliance@one.verizon.com

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions (Verizon)

Audit Protocol

1. Background

- 1.1 The purpose of Verizon's Binding Corporate Rules Controller Policy and Binding Corporate Rules Processor Policy (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") is to safeguard personal information transferred between the Verizon group members ("**Group Members**").
- 1.2 The Policies require approval from the data protection authorities in the European Member States from which the personal information is transferred. One of the requirements of the data protection authorities is that Verizon audits compliance with the Policies and satisfies certain conditions in so doing and this document describes how Verizon deals with such requirements.
- 1.3 The role of Verizon's Director, Privacy Policy & Compliance International in the EU headquarters in the UK and the network of Regulatory Officers is to provide guidance about the collection and use of personal information subject to the Policies and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use of personal information is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Verizon to ensure compliance with the Policies as required by the data protection authorities, this is only one way in which Verizon ensures that the provisions of the Policy are observed and corrective actions taken as required.

2. Approach

- 2.1 Overview of audit
 - 2.1.1 Compliance with the Policies is overseen on a day to day basis by the Director, Privacy Policy & Compliance International.
 - 2.1.2 The Internal Audit Department will be responsible for performing and/or overseeing independent audits of compliance with the Policies and will ensure that such audits address all aspects of the Policies. The Internal Audit Department will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of the Director, Privacy Policy & Compliance International and that any corrective actions to ensure compliance take place within a reasonable timescale.

- 2.1.3 To the extent that Verizon acts as a processor, audits of compliance with the commitments made in the Processor Policy may also be carried out by or on behalf of Verizon's customers in accordance with the terms of a contract Verizon has with a customers in respect of such processing, and such audits may also extend to any sub-processors acting on Verizon's behalf in respect of such processing and the ability to audit such sub-processors will be carried out in accordance with the terms of the contract between Verizon and the sub-processors.
- 2.2 Timing and scope of audit
 - 2.2.1 Audit of the Policy will take place:
 - (a) annually in accordance with Verizon's audit procedure/s; and/or
 - (b) more frequently at the request of the Director, Privacy Policy & Compliance International and/or as determined necessary by the Executive Director, Legal & Regulatory Affairs in the EU.
 - 2.2.2 To the extent that a Group Member processes personal information on behalf of a third party controller, audit of the Processor Policy will take place as required under the contract in place between that Group Member and that third party controller.
 - 2.2.3 The scope of the audit performed will be determined by the Internal Audit Department based on a risk-based analysis which will consider relevant criteria, for example: areas of known non-compliance, areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature, method and location of the personal information processed.
 - 2.2.4 In the event that a third party controller on whose behalf Verizon processes personal information exercises its right to audit Verizon for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, files, documents (where appropriate) and activities relating to that controller. Verizon will not provide a controller with access to systems which process personal information of other controllers.
- 2.3 Auditors
 - 2.3.1 Audit of the procedures and controls in place to give effect to the commitments made in the Policies will be undertaken by Verizon's Internal Audit Department and Verizon may use other accredited internal/external auditors as determined by Verizon.
 - 2.3.2 In the event that a third party controller on whose behalf Verizon processes personal information exercises their right to audit Verizon for compliance with the Processor Policy, such audit may be

undertaken by that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between Verizon and that controller.

2.4 Report

On completion of the audit the report and findings will be made available to the Director, Privacy Policy & Compliance International and the Executive Director, Legal & Regulatory Affairs Europe responsible for the EU. A summary of the findings will be provided to the EU Management Committee with details of any remedial action required, recommendations and timescales for remedial action to be undertaken.

2.4.1 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Verizon has agreed to:

- (a) provide copies of the results of any audit of the Policies to a European data protection authority of competent jurisdiction; and
- (b) to the extent that an audit relates to personal information processed by Verizon on behalf of a third party controller, to make the results of any audit of compliance with the Processor Policy available to that controller.

2.4.2 Verizon's Director, Privacy Policy & Compliance International will be responsible for liaising with the European data protection authorities for the purpose of providing the information outlined in section 2.4.11.

2.4.3 In addition Verizon has agreed that European data protection authorities may audit Group Members for the purpose of reviewing compliance with the Policies in accordance with the terms of the Co-operation Procedure which is attached as Appendix 6 of the Binding Corporate Rules Controller Policy and of the Binding Corporate Rules Processor Policy of Verizon.

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions (Verizon)

Complaint Handling Procedure

1. Introduction

- 1.1 The Binding Corporate Rules Controller Policy ("**Controller Policy**") and the Binding Corporate Rules Processor Policy ("**Processor Policy**") (together the "**Policies**") safeguard personal information transferred between the Verizon group members ("**Group Members**"). The content of the Policies is determined by the data protection authorities in the European Member States from which the personal information is transferred and one of their requirements is that Verizon must have a complaint handling procedure in place. The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Verizon under the Policies are dealt with.

2. How individuals can bring complaints

- 2.1 All complaints made under the Policies whether Verizon is collecting and/or using personal information on its own behalf or on behalf of a customer can be brought in writing to Verizon's Director, Privacy Policy & Compliance International at emeadataprotection@intl.verizon.com.

3. Who handles complaints?

3.1 Complaints where Verizon is a controller

- 3.1.1 Verizon's Director, Privacy Policy & Compliance International will handle all complaints arising under the Controller Policy in respect of the collection and use of personal information where Verizon is the controller of that information. Verizon's Director, Privacy Policy & Compliance International will liaise with relevant business units to investigate the complaint. The Director, Privacy Policy & Compliance International will coordinate a response.

3.1.2 What is the response time?

Verizon's Director, Privacy Policy & Compliance International will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, Verizon's Director, Privacy Policy & Compliance International will advise the complainant accordingly and provide a reasonable

estimate (not exceeding six months) for the timescale within which a response will be provided.

3.1.3 When a complainant disputes a finding

If the complainant disputes the response of the Director, Privacy Policy & Compliance International (or the individual or department within Verizon dealing with the complaint) or any aspect of a finding, and notifies Verizon accordingly, the matter will be referred to the Executive Director, Legal & Regulatory Affairs Europe ("**Executive Director**") who will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Executive Director will respond to the complainant within six months of the referral. If the complaint is upheld, the Executive Director will arrange for any necessary steps to be taken as a consequence.

3.1.4 Individuals whose personal information is processed in accordance with European data protection law also have the right to complain to a European data protection authority and/or to lodge a claim with a court of competent jurisdiction and this will apply whether or not they have first made a complaint to Verizon.

3.1.5 The jurisdiction from which the personal information was transferred will determine to which data protection authority a complaint may be made.

3.1.6 If the matter relates to personal information which has been exported to a Group Member outside Europe and an individual wants to make a claim against Verizon, the claim may be made against Verizon UK in the UK or in the country of the Group Member in Europe responsible for exporting the personal information.

3.2 Complaints where Verizon is a processor

3.2.1 Where a complaint arises under the Processor Policy in respect of the collection and use of personal information where Verizon is the processor in respect of that information, Verizon will communicate the details of the complaint to the customer promptly and will act strictly in accordance with the terms of the contract between the customer and Verizon if the customer requires Verizon to deal with the complaint.

3.2.2 When a customer ceases to exist

In circumstances where a customer has disappeared, no longer exists or has become insolvent, individuals whose personal information is collected and/or used in accordance with European data protection law and transferred between Group Members on behalf of that customer under the Processor Policy have the right to complain to Verizon and Verizon will

deal with such complaints in accordance with section 3.1 of this Complaint Handling Procedure. In such cases, individuals also have the right to complain to a European data protection authority and/or to lodge a claim with a court of competent jurisdiction and this will apply whether or not they have first made a complaint to Verizon.

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions ("Verizon")

Co-operation Procedure

1. Introduction

- 1.1 This Co-operation Procedure sets out the way in which Verizon will co-operate with the European¹ data protection authorities in relation to the Binding Corporate Rules Controller Policy and the Binding Corporate Rules Processor Policy (together the "**Policies**").

2. Co-operation Procedure

- 2.1 Where required, Verizon will make the necessary personnel available for dialogue with a European data protection authority in relation to the Policies.
- 2.2 Verizon will actively review and consider:
- (a) any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Policies; and
 - (b) the views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules for data controllers and Binding Corporate Rules for data processors.
- 2.3 Subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Verizon will provide upon request copies of the results of any audit of the Policies to a relevant European data protection authority.
- 2.4 Verizon agrees that:
- 2.4.1 where any Verizon group member ("**Group Member**") is located within the jurisdiction of a data protection authority based in Europe, Verizon agrees that that particular data protection authority may audit that Group Member for the purpose of reviewing compliance with the

¹ References to Europe for the purposes of this document means the EEA and Switzerland

Policies, in accordance with the applicable law of the country in which the Group Member is located; and

- 2.4.2 in the case of a Group Member located outside Europe, Verizon agrees that a data protection authority based in Europe may audit that Group Member for the purpose of reviewing compliance with the Policy in accordance with the applicable law of the European country from which the personal information is transferred under the Policies (which, when Verizon acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller) on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Verizon (unless this requirement is in conflict with local applicable law).
- 2.5 Verizon agrees to abide by a formal decision of the applicable data protection authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

Binding Corporate Rules Controller and Binding Corporate Rules Processor of Verizon Enterprise Solutions ("Verizon")

Updating Procedure

1. Introduction

- 1.1 This Binding Corporate Rules Updating Procedure sets out the way in which Verizon will communicate changes to the Binding Corporate Rules Controller Policy ("**Controller Policy**") and to the Binding Corporate Rules Processor Policy ("**Processor Policy**") (together the "**Policies**") to the European¹ data protection authorities, data subjects, its customers and to the Verizon group members ("**Group Members**") bound by the Policies.

2. Material changes to the Policies

- 2.1 Verizon will communicate any material changes to the Policies as soon as is reasonably practical to the Information Commissioner's Office and to any other relevant European data protection authorities.
- 2.2 Where a change to the Processor Policy affects the conditions under which Verizon processes personal information on behalf of any customer, Verizon will also communicate such information to any affected customer before it is implemented, and with sufficient notice to enable affected customers to object. Verizon's customer may then suspend the transfer of personal information to Verizon and/or terminate the contract, in accordance with the terms of its contract with Verizon.

3. Administrative changes to the Policies

- 3.1 Verizon will communicate changes to the Policies which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure to the Information Commissioner's Office and to any other relevant European data protection authorities at least once a year. Verizon will also provide a brief explanation to the Information Commissioner's Office and to any other relevant data protection authorities of the reasons for any notified changes to the Policies.
- 3.2 Verizon will make available changes to the Processor Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative,

¹ References to Europe for the purposes of this document includes the EEA and Switzerland

court or supervisory authority measure to any customer on whose behalf Verizon processes personal information.

4. Communicating and logging changes to the Policies

- 4.1 The Policies contain a change log which sets out the date of revisions to the Policies and the details of any revisions made. Verizon's Director, Privacy Policy & Compliance International will maintain an up to date list of the changes made to the Policies.
- 4.2 Verizon will communicate all changes to the Policies, whether administrative or material in nature:
 - 4.2.1 to the Group Members bound by the Policies; and
 - 4.2.2 systematically to customers on whose behalf Verizon processes personal information and to the data subjects who benefit from the Policies via the Verizon website www.verizon.com/privacy.
- 4.3 Verizon's Director, Privacy Policy & Compliance International will maintain an up to date list of the changes made to the Policies, the list of Group Members bound by the Policies and a list of the sub-processors appointed by Verizon to process personal information on behalf of its customers. This information will be available on request from Verizon.

5. New Group Members

- 5.1 Verizon's Director, Privacy Policy & Compliance International will ensure that all new Group Members are bound by the Policies before a transfer of personal information to them takes place.