VERIZON BUSINESS GROUP

EU BINDING CORPORATE RULES PROCESSOR POLICY

Updated February 2023

CONTENTS

Confidential

INTRODUCTION TO THIS POLICY

This EU Binding Corporate Rules Processor Policy and its Appendices (together the "**Policy**") establish the approach taken by Verizon Business Group (previously referred to as Verizon Enterprise Solutions) ("**Verizon**") to the protection and management of personal information globally by Verizon EU BCR - Processor group members ("**Group Members**") when processing that information on behalf of a controller Third Party established in Europe.

Verizon provides a cloud based platform to deliver IT, security, mobility and managed solutions to corporate and government customers. It has a global network that reaches more than 150 countries, with Verizon Communications, Inc. as parent company.

In addition to other definitions provided under this Policy, the following further terms shall have the meanings ascribed to them below. Terms not defined below or elsewhere in this Policy shall have the meaning given them in the GDPR:

"**competent supervisory authority**" means a supervisory authority which has jurisdiction in relation to the activities of a controller or processor under European data protection law in a particular Member State;

"**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information;

"**customer**" means a controller Third Party for which a Group Member provides a service;

"**customer personal information**" means any personal information which Group Members process on behalf of a customer (controller) and which relates to an identified or identifiable natural person who ultimately benefits from or makes use of the services contracted by the customer (an end-user). Customer personal information does not include personal information for the operation of the service (i.e. billing data), which is processed by Group Members in their capacity as controllers and is therefore excluded from this Policy;

"**data processing agreement**" means a contract or any other type of legal instrument containing data processing terms and conditions;

"**Europe**" means the countries in the European Economic Area ("**EEA**") plus Switzerland;

"**European data protection law**" means the GDPR and any data protection law of a European Member State and Switzerland, including local legislation implementing the requirements of the GDPR, including subordinate legislation, in each case as amended from time to time;

"**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation);

"**lead supervisory authority**" means, for the purposes of this Policy, the Irish supervisory authority known as the Data Protection Commission;

"Local Data Protection Law" means any applicable local data protection law.

"**personal information**" means any personal information subject to European data protection law which relates to an identified or identifiable natural person, being one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number,

location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**processing**" means any operation or set of operations which Verizon performs on personal information or on sets of personal information, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, uses, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**processor**" means a natural or legal person, public authority, agency or another body which processes personal information on behalf of the controller;

"**supervisory authority**" means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR; and

"**Third Party**" means a natural or legal person, public authority, agency or other body which is not a Group Member.

This Policy applies to all customer personal information processed by Group Members as processors and/or sub-processors as part of their regular business activities in the course of providing services to a customer established in Europe or otherwise subject to the GDPR.

Group Members and their employees must comply with and respect this Policy when processing customer personal information in their capacity as service providers to a customer.

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 https://www.verizon.com/about/privacy/binding-corporate-rules.

Confidential

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 processed. Under European data protection law, when an organisation processes 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, 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 Verizon provides services to customers as a global telecommunications provider, Verizon will be acting as a processor in respect of the customer personal information.

HOW DOES DATA PROTECTION LAW AFFECT VERIZON INTERNATIONALLY?

European data protection law does not allow the transfer of personal information to countries outside Europe that do not ensure an adequate level of data protection. Some of the countries in which Verizon operates do not provide an adequate level of protection for individuals' data privacy rights under European data protection law.

When Verizon acts as a processor to a customer, Verizon's European customers retain the responsibility to comply with European data protection law. In practical terms, this means that those acting as controllers (i.e. customers) must pass certain data protection obligations onto any processor which processes customer 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 European 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 Ireland Limited to show that the Group Member outside Europe (or a Third Party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place. In addition, a customer that has entered into a data processing agreement with Verizon that incorporates this Policy may enforce this Policy in the European courts, where permitted by law and subject to the terms of the data processing agreement, against (i) any Group Member processing customer personal information on behalf of that customer in respect of a breach of the Policy caused by that Group Member; and (ii) the Group Member which exported customer personal information to the Group Member in (i), so long as that Group Member exporting customer personal information is located in Europe; or (iii) in those cases where it is not possible to bring a claim against a Group Member in Europe, claims may be made against Verizon Ireland Limited.

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 customer personal information transferred to and processed by Group Members as processors or sub-processors.

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 customer personal information transferred to Group Members under the terms of its contract with Verizon, Verizon will apply this Policy whenever a Group Member processes customer personal information as a processor. Where Verizon's customers rely upon this Policy as providing adequate safeguards, a link to 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 customer personal information.

Verizon will apply this Policy globally where Group Members process customer 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 is legally binding and applies to all Group Members and their employees where those Group Members process customer personal information as a processor both manually and by automatic means, and requires that Group Members who collect, process or transfer customer personal information to provide services to a customer 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 (and their employees) must comply with the EU Binding Corporate Rules Controller Policy when they process personal information as a controller, or whenever they act as a processor for a controller which is a Group Member. Some Group Members may act as a controller/processor for another Group Member and as a processor for a Third Party, and must therefore comply with this Policy and also the EU Binding Corporate Rules Controller Policy as appropriate.

WHAT PERSONAL INFORMATION DOES THIS POLICY COVER?

Personal information processed under this Policy includes customer personal information, including data stored and transmitted across the Verizon network in performing communication services under contracts with customers, such as call detail records, IP addresses, IP network information and geolocation traffic.

FOR WHAT PURPOSES IS PERSONAL INFORMATION TRANSFERRED UNDER THIS POLICY?

Transfers of customer personal information under this Policy (including to United States, the Philippines and India) may take place for the purposes of provisioning of services to customers, including call details records in provisioning of services, IP traffic residing in data centres for the purpose of hosting and cloud services, or IP traffic processed in data centres outside Europe for the purposes of providing Managed Security Services.

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, International Privacy at the address below, who will either deal with the matter or forward it to the appropriate person or department within Verizon.

Attention:	**Director, International Privacy**
Email:	**EMEAdataprotection@verizon.com**
Telephone:	**+353 01 246 8000**
Address:	**Verizon, 2nd Floor Boru House Block T, East Point Business Park, Dublin DO3 R6C6, Republic of Ireland**

The Director, International Privacy is responsible for ensuring that changes to this Policy are notified in accordance with Appendix 7.

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

Confidential

PART II: PROCESSOR OBLIGATIONS

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles that Group Members must observe when they process customer personal information as a processor.
- Section B deals with the practical commitments made by Group Members to the supervisory authorities when they process customer personal information as a processor on behalf of a customer.
- Section C describes the third party beneficiary rights that Group Members have granted to individuals in its capacity as a processor under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS AND FAIRNESS

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

Where this Policy applies and:

- Local Data Protection Law requires a higher level of protection than is provided for in this Policy, Group Members acknowledge that it will take precedence over this Policy; or
- local applicable law prevents a Group Member from fulfilling, or has a substantial effect on its ability to comply with its obligations under this Policy, that Group Member will follow the process set out in Rule 12.

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

Group Members will, taking into account the nature of processing and information available to them, within a reasonable time and to the extent reasonably possible, and as may be required under data processing agreements with its customers, assist customers on request to comply with their obligations as controllers under European data protection law. For example, Group Members will be transparent about sub-processor activities so that their customers may correctly inform individuals.

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

Rule 2A – Group Members will assist customers to comply with the requirement to explain to individuals at the time their customer personal information is collected how that information will be processed.

Group Members' customers have a duty to explain to individuals, at the time their customer personal information is collected, how that information will be processed. Group Members will provide such assistance and information to their customers as may be required under the terms of its data processing agreements with their customers to comply with this requirement, for example, information about any sub-processors appointed by the Group Member to process customer personal information on its behalf.

Rule 2B – Group Members will only process customer personal information on behalf of and in accordance with the instructions of the customer.

Group Members and their employees will respect the Policy and only process customer personal information in compliance with the terms of the data processing agreement they have with their customers in relation to such processing, and which contain the terms required by European data protection law in so far as they relate to the engagement of a processor, including in relation to transfers of customer personal information to destinations outside Europe, unless required to do so by European laws to which the Group Member is subject. In such a case, the Group Member will inform the customer of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest.

Group Members will immediately inform their customers if, in their opinion, an instruction infringes European data protection law.

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

On the termination of the provision of the services related to data processing to a customer, Group Members and their sub-processors will act in accordance with the instructions of the customer and return, destroy or store the customer personal information, including any copies of the customer personal information, in a secure manner or as otherwise required by the customer. If the Group Member and its sub-processors are required to destroy the customer personal information, upon request from the customer, they will certify that they have deleted any copies of the customer personal information.

In the event that Member State law prevents a Group Member from returning the customer personal information to a customer or destroying it, that Group Member will ensure that such information remains confidential and will not process the customer personal information otherwise than in accordance with the instructions of the customer or as required by applicable law.

RULE 3 – ENSURING DATA QUALITY

Rule 3 – Group Members will assist customers to keep the customer personal information accurate and up to date to the extent reasonably possible.

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

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

Group Members will notify other Group Members or any Third Party sub-processor to whom customer personal information has been disclosed accordingly so that they can update their records.

In practice, when Group Members act for a customer in their capacity as a cloud provider, Group Members do not have access to the customer personal information of their customers and so, when acting in this capacity, Group Members will not be required to delete, anonymise, update or correct such customer personal information.

Confidential

RULE 4 – HONOURING INDIVIDUAL RIGHTS

Rule 4 – Group Members will assist customers to comply with the rights of individuals.

Group Members will act in accordance with the instructions of their customers and undertake any appropriate technical and organisational measures to enable their customers to comply with their duty to respect the rights of individuals. In particular, if any Group Member receives a request from an individual exercising their rights, the Group Member will transfer such request promptly to the relevant customer and not respond to such a request unless authorised to do so. Group Members will follow the steps set out in section 6 of the Individuals' Rights Procedure (see Appendix 1).

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – Group Members will implement appropriate technical and organisational security measures required by European data protection law.

Where Group Members provide a service to a customer which involves the processing of customer personal information, the contract between the Group Member and its customer imposes clear obligations dealing with the security of that information which will at least meet the requirements of European data protection law to ensure that Verizon has in place appropriate technical and organisational security measures to ensure a level of security to customer personal information appropriate to the risk presented by the processing.

Group Members will adhere to the security and organisational measures specified in contracts with their customers, and will assist customers in implementing appropriate technical and organisational security measures to facilitate compliance with this Policy in practice (such as data protection by design and by default) so far as is reasonable taking into account the state of the art, cost of implementation, risks to individuals, nature, scope, context and purpose of the processing.

Rule 5B – Group Members will notify customers of any Data Protection Breach.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, customer personal information transmitted, stored or otherwise processed (a "**Data Protection Breach**"), the person who becomes aware of the breach within the relevant Group Member will, without undue delay, notify databreachreport@one.verizon.com which is managed by the Director, International Privacy and the commercial legal, regulatory and security team (the "**Data Breach Panel**"). The Data Breach Panel will analyse the details of the Data Protection Breach and notify the customer without undue delay and in accordance with the terms of its contract with that customer.

If sub-processors are appointed in accordance with Rule 5C below, sub-processors will inform the customer and the processor Group Member of any Data Protection Breach without undue delay.

Data Protection Breaches suffered by Group Members and Third Party sub-processors, and the facts, the effects of such incidents and the remedial action taken, will be documented in a Data Protection Breach report which will be available to the customer on request.

Rule 5C – Group Members will comply with the requirements of a customer regarding the appointment of any internal and external sub-processor.

Group Members will inform their customers where processing undertaken on their behalf will be conducted by an internal and external 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, and in particular will obtain prior informed specific or general written authorisation of the customer regarding the appointment of any sub-processors.

Where the customer has provided general written authorisation, Group Members will ensure that up to date information regarding its appointment of sub-processors is available to those customers at all times so that customers have the opportunity to object 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 customer personal information on its behalf, that customer will be entitled to take such steps as are consistent with the terms of its contract with the Group Member and as referred to in Rule 2B of Part II of this Policy (i.e. the Group Member's customer may then suspend the transfer of customer personal information to Verizon and/or terminate the contract, depending upon the terms of its contract with the Group Member).

Rule 5D – Group Members will ensure that internal and external 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 internal and external sub-processors who provide sufficient guarantees in respect of the commitments made by Group Members in this Policy. In particular, such sub-processors must be able to provide sufficient guarantees to implement appropriate technical and organisational measures that will govern their processing of the customer personal information to which they will have access in such a manner that the processing will meet the requirements of European data protection law.

To comply with this Rule, where a sub-processor has access to customer personal information covered by this Policy, Group Members will impose strict contractual obligations in writing on the sub-processor in accordance with the terms of the Group Member's contract with its customer. Those requirements include:

- commitments on the part of the sub-processor regarding its assistance in the compliance with European data protection law, data quality, transparency and purpose limitation principles, individuals' rights and security of that information, consistent with those contained in this Policy (and in particular, and without limitation, Rules 1, 2A, 2B, 3, 4, 5A and 5B above) and with the terms of the contract the Group Member has with its customer in respect of the processing in question;
- that the sub-processor will act only on the Group Member's instructions when processing customer personal information;
- adequate safeguards (as understood in European data protection law) with respect to transfers of customer personal information to a Third Party sub-processor established in a country outside Europe that supervisory authorities do not consider ensures an adequate level of protection for individuals' data privacy rights;
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by the Group Members in this Policy as may be applicable to sub-processors; and
- that where the sub-processor fails to fulfil its data protection obligations, the Group Members will remain fully liable to the customer for the performance of the sub-processor's obligations.

SECTION B: PRACTICAL COMMITMENTS

RULE 6 – COMPLIANCE AND ACCOUNTABILITY

Rule 6A – Group Members will have appropriate staff and support to ensure and oversee privacy compliance with this Policy throughout the business and will make available to the customer all necessary information to demonstrate compliance.

Verizon has appointed its Director, International Privacy 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 6B – Group Members processing customer personal information will maintain a written (including in electronic form) record of their processing activities and make that record available to competent supervisory authorities on request.

The data processing records maintained by Group Members will contain:

- the Group Member's name and contact details;
- the name and contact details of each customer on whose behalf the Group Member processes customer personal information and, where applicable, the customer's representative and data protection officer;
- the categories of processing carried out on behalf of each customer;
- details of the third country or countries to which customer personal information is transferred, including the identification of that third country or international organisation and the documentation of suitable safeguards in the event of transfers under the second subparagraph of Article 49(1) of the GDPR; and
- where possible, a general description of the technical and organisational security measures used to protect customer personal information.

RULE 7 – TRAINING

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

RULE 8 – AUDIT

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

RULE 9– COMPLAINT HANDLING

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

RULE 10 – COOPERATION WITH SUPERVISORY AUTHORITIES

Confidential

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

RULE 11 – UPDATE OF THE POLICY

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

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

Rule 12A - Group Members will carry out a transfer impact assessment before making transfers under this Policy.

European Group Members will carry out a transfer impact assessment to assess if the legislation applicable to them prevents them from fulfilling their obligations under this Policy, or has a substantial effect on the guarantees provided under this Policy before making transfers of customer personal information under this Policy. The transfer impact assessment, which shall be documented and made available to the competent supervisory authority upon request, must take into account:

- the specific circumstances of the transfer such as the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred customer personal information; the economic sector in which the transfer occurs; and the storage location of the data transferred; and

- the laws and practices of the third country (including the possibility of legal access requests by public authorities) relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards.

If it is assessed that any safeguards in addition to those envisaged under this Policy should be put in place, Verizon Ireland Limited and the Director, International Privacy will be informed and involved in the transfer impact assessment.

After carrying out a transfer impact assessment, Group Members will be informed that the assessment has been carried out and of the results of the transfer impact assessment so that the identified additional safeguards will be applied where a Group Member carries out the same type of transfer.

Where additional safeguards could not be put in place, the European Group Member shall promptly notify the customer, and the customer will be entitled to suspend the transfer of customer personal information and/or terminate the contract with the Group Member, as provided for in Rule 2B. If the transfers are suspended, any customer personal information transferred prior to the suspension will be, at the request of the customer, destroyed or returned to the customer.

Rule 12B – Group Members will ensure that where they believe that the legislation applicable to them prevents them from fulfilling the instructions received from the customer or their obligations under this Policy or contract with the customer, that Group Member will promptly inform (unless otherwise prohibited by law):

- **the customer, who will be entitled to suspend the transfer of customer personal information and/or terminate the contract with the Group Member, as provided for in Rule 2B;**
- **Verizon's Director, International Privacy;**
- **Verizon Ireland Limited; and**
- **the supervisory authority competent for the customer and the processor.**

In addition to the above:

- Group Members outside Europe will notify European Group Members and the customer where there is a change in the laws of the third country which could affect the results of the initial transfer impact assessment carried in accordance with Rule 12A. Following such a notification, the European Group Member shall promptly identify appropriate measures to be adopted by the European Group Member and/or the Group Member outside Europe to address the situation. Where appropriate measures cannot be ensured, or if so instructed by the competent supervisory authority, the customer will be entitled either to suspend the transfer of customer personal information and/or terminate the contract with the Group Member, as provided for in Rule 2B.

- European Group Members will monitor, on an ongoing basis, any developments in the third countries which could affect the results of the initial transfer impact assessment carried out in accordance with Rule 12A.

Rule 12C – Group Members will ensure that where they receive a legally binding request from a law enforcement agency or state security body for disclosure of customer personal information transferred outside Europe under this Policy, that Group Member will, unless prohibited from doing so by the requesting authority:

- **put the request on hold; and**
- **promptly notify the customer and the supervisory authority competent for each of the customer and the processor.**

Where Group Members outside Europe receive a legally binding request for disclosure of information transferred outside Europe under this Policy and are prohibited by a law enforcement authority from putting the request on hold and/or from notifying the competent supervisory authorities, Group Members will:

- use their best efforts to obtain a waiver of this prohibition in order to communicate as much information as they can and as soon as possible to the competent supervisory authorities; and
- demonstrate to the competent supervisory authorities the steps they followed to deal with the request in accordance with this Policy.

Group Members will provide to the competent supervisory authorities on an annual basis general information about the nature and number of such requests that it receives, type of data requested and the requesting body if possible.

In any event, Group Members will ensure that any transfers of customer personal information under this Policy that it makes to a public authority are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Confidential

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

(a) Where customer personal information is processed under this Policy by a European Group Member acting as a processor under a data processing agreement with a customer, that individual whose customer personal information is transferred under the terms of that data processing agreement to a Group Member outside Europe, will have the rights as third party beneficiaries to enforce Rules 1B, 2, 3, 4, 5, 9, 10, 12, the right to access the Policy via https://www.verizon.com/about/privacy/binding-corporate-rules , or to obtain a hard copy of the Policy as well as a list of the Group Members bound by this Policy, and the right to enforce the provisions in Section C (a), (c), (d), (e), (f), (g) and (h) granting third -party beneficiary rights and setting the liability and jurisdiction rules under the Policy.

(b) Where customer personal information is processed under this Policy by a European Group Member acting as a processor under a data processing agreement with a customer and where:

(i) the individual whose customer personal information is transferred as described in (a) above is unable to bring a claim against the customer because the customer 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 customer by contract or by operation of law, that individual will have the rights as third party beneficiary to enforce Rules 1B, 2, 3, 4, 5, 9, 10, 12, the right to access the Policy via https://www.verizon.com/about/privacy/binding-corporate-rules, or to obtain a hard copy of the Policy as well as a list of the Group Members bound by this Policy, and the right to enforce the provisions in Section C (b), (c), (d), (e), (f)(g) and (h) granting third-party beneficiary rights and setting the liability and jurisdiction rules under the Policy.

(c) This Policy ensures that the individuals referred to in Section C (a) and (b) above are able to enforce the rights outlined in those sections by:

(i) *making complaints*: individuals may make complaints to a Group Member (in accordance with the Complaint Handling Procedure set out in Appendix 5) and to the competent supervisory authority in the Member State in which the alleged infringement took place, or in which the individual works or habitually resides; and/or

(ii) *bringing proceedings* against Verizon Ireland Limited in the courts of a Member State in which the relevant customer or Verizon has an establishment, or in the Member State in which the individual has his habitual residence.

(d) Where the Group Member and the customer involved in the same processing are found responsible for any damage caused by such processing, the individuals referred to in Section C (a) and (b) above will be entitled to receive compensation for the entire damage directly from the Group Member.

(e) The individuals referred to in Section C (a) and (b) above may also seek appropriate redress from Verizon Ireland Limited including the remedy of any breach of the provisions in those sections, and where appropriate, receive compensation from Verizon Ireland Limited for the entirety of any damage whether material or non-material suffered as a result of a breach of those provisions by:

(i) any Group Member outside Europe acting as a processor; or

(ii) any Third Party sub-processor which is established outside Europe and which is acting on behalf of Verizon,

in accordance with the determination of a court or other competent authority.

(f) Verizon Ireland Limited will ensure that any necessary action is taken to remedy any breach of this Policy by a Group Member outside Europe or any Third Party sub-processor which is established outside Europe and which is processing customer personal information on behalf of a customer.

(g) For the avoidance of doubt, individuals shall benefit from the third party beneficiary rights as described in this Section C and the European courts or competent supervisory authorities shall have jurisdiction as if the breach of the provisions described in this Section C or any of them was caused by Verizon Ireland Limited in the Republic of Ireland. Verizon Ireland Limited may not rely on a breach by a sub-processor (internal or external) of its obligations in order to avoid its own liabilities.

(h) In the event of a claim being made under this Section C in which an individual has suffered damage as described above and where that individual can demonstrate that it is likely that the damage has occurred because a breach of this Policy, Verizon has agreed that the burden of proof to show that a Group Member outside Europe (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 Ireland Limited.

PART III: APPENDICES

Confidential

Appendix 1

EU Individuals' Rights Procedure

1. **INTRODUCTION**

1.1 When a Group Member processes personal information for their own purposes, the Group Member is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the requirements of European data protection law in relation to the exercise of individuals' rights.

1.2 All individuals whose personal information is processed by a Group Member acting as controller, and transferred between Group Members within the scope of the EU Binding Corporate Rules Controller Policy have the right to:

(a) be informed by the Group Member whether any personal information about them is being processed by the Group Member and, if the Group Member does process their personal information, they are entitled to access it (this is known as the right of **access**); and

(b) rectify, erase, restrict, port and/or object to the processing of their personal information.

1.3 Requests to exercise these rights will be dealt with in accordance with the terms of this Individuals' Rights Procedure ("**Procedure**").

1.4 This Procedure explains how Group Members deal with requests relating to personal information that fall into the categories in section 1.2 above (referred to as "valid requests" in this Procedure). Where Local Data Protection Law differs from this Procedure and requires a higher level of protection for personal data, the law which affords the higher level of protection will prevail.

1.5 Information about how individuals may exercise the rights described in section 1.2 above is also set out in the fair processing statements provided to individuals by Group Members.

1.6 Requests from individuals relating to the rights described in section 1.2 above may be made via the Verizon website at https://www.verizon.com/about/privacy/data-subject-rights, or by email to emeadataprotection@verizon.com. Where requested by the individual, Verizon will provide the information orally, provided that the identity of the individual is proven by other means.

2. **INDIVIDUALS' RIGHTS**

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

(a) be informed whether the Group Member is processing personal information about that individual;

(b) be given a description of:

(i) the purpose for which the personal information is being processed and the categories of personal information concerned;

(ii) the recipients or categories of recipients to whom the information is, or may be, disclosed by Group Members, including recipients located outside Europe;

(iii) the period for which the personal information will be stored, or the criteria used to determine that period;

(iv) the existence of the rights to rectification, erasure, restriction of and to object to processing and to complain to a supervisory authority;

(v) the source of the personal information and the categories of personal information concerned, if it was not collected from the individual;

(vi) the safeguards in place where personal information is transferred from Europe to a third country;

(vii) the logic involved in (to the extent required by applicable law) and the significance and consequences of any decision-making undertaken by automatic means, including profiling;

(c) be provided with a copy of the personal information held by Group Members. If the request is made by email, the information shall be provided via email, unless the individual making the request indicates otherwise;

(d) require the rectification, erasure, restriction and portability of their personal information;

(e) not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similar significant effects; and/or

(f) object to the processing of his or her personal information.

3. **RECEIVING A REQUEST**

3.1 If a Group Member, including a Non-European Group Member, receives any request from an individual relating to the rights described in section 1.2 above, this must be passed to the Director, International Privacy immediately upon receipt indicating the date on which it was received together with any other information which may assist the Director, International Privacy to deal with the request. Such requests can be sent to emeadataprotection@verizon.com.

3.2 The Director, International Privacy 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. The request does not have to be official or mention data protection law to qualify as a valid request.

3.3 When the individual making the valid request is not an employee of a Group Member and the Group Member has reasonable doubts concerning the identity of the individual, the Group Member may request such information that it may reasonably require in order to confirm the identity of the individual making the request.

3.4 Group Members must deal with a valid request without undue delay and in any event within 1 month of its receipt. Group Members may extend this period, by up to two further months if necessary, taking into account the complexity and number of the requests. Where a Group Member extends the period in which it will deal with a valid request, the Group Member will inform the individual of the extension within one month of receipt of their request, together with the reasons for the delay.

3.5 The Director, International Privacy will contact the individual in writing to confirm receipt of the valid request, seek confirmation of identity or further information (e.g. clarification on the processing activities to which the request relates), if required, or decline the request in accordance with section 4 below.

4. DECLINING VALID REQUESTS

4.1 A valid request may be refused on the following grounds:

(a) where the request is made to a European Group Member and relates to the processing of personal information by that Group Member, if:

(i) the refusal is consistent with the data protection law within the Member State in which that Group Member is located; or

(ii) the Group Member demonstrates that the request is manifestly unfounded or excessive; or

(b) where the valid request is made to a non-European Group Member and the Director, International Privacy is unable to deal with the request in accordance with section 3, the relevant non-European Group Member will only refuse the request if the grounds for such refusal are consistent with the data protection law within the European Member State from which the personal information was transferred.

4.2 The Group Member will inform the individual of the refusal of the request within one month of the receipt of the request and of the individual's right to complain to a competent supervisory authority or seek a judicial remedy in relation to the refusal.

5. GROUP MEMBER'S RESPONSE

5.1 The Director, International Privacy will arrange a search of all electronic and paper filing systems relevant to the request.

5.2 The Director, International Privacy may refer any complex cases to the Chief Privacy Officer 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 Where the valid request is a request for subject access, the information requested will be collated by the Director, International Privacy into a readily understandable format (internal codes or identification numbers used by Group Members that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Director, International Privacy which includes information required to be provided in response to the valid request.

5.4 If the valid request is for the erasure, rectification, restriction or portability of personal data, or is an objection to processing or relates to the right not to be subject to automated decision-making where the Group Member is the controller for that personal information, such a request must be considered and dealt with as appropriate by the Director, International Privacy. In particular:

(a) if the valid request is advising of a change or any inaccuracy in an individual's personal information, where the Group Member is the controller for that personal

information, such information must be rectified or updated accordingly if the Group Member is satisfied that there is a legitimate basis for doing so;

(b) when, pursuant to a valid request, a Group Member erases, anonymises, updates, corrects or restricts the processing of personal information, either in its capacity as controller or on instruction of a customer when it is acting as a processor in accordance with section 6 below, that Group Member 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; and

(c) if the valid request made to a Group Member as a controller is to erase that individual's personal information in accordance with the provisions of applicable European data protection law, the matter will be assessed by the Director, International Privacy. Where the processing undertaken by the Group Member is required or permitted by law, or is necessary for the exercising of the right of freedom of expression and information, the request will be refused.

5.5 All queries relating to this Procedure are to be addressed to the Director, International Privacy.

6. REQUESTS MADE TO A GROUP MEMBER WHERE THE GROUP MEMBER IS A PROCESSOR

6.1 When a Group Member processes information on behalf of a customer (for example, to provide a service) the Group Member is deemed to be a processor of the information and the customer will be primarily responsible for meeting the legal requirements under European data protection law as a controller. This means that when a Group Member acts as a processor, Verizon's customer retains the responsibility to comply with European data protection law.

6.2 Certain data protection obligations are passed to Verizon in the contracts which 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 request from an individual to exercise his or her rights under European data protection law in the Group Member's capacity as a processor on behalf of a customer, that Group Member must transfer such request promptly to the relevant customer and not respond to the request unless authorised by the customer to do so.

6.3 When a Group Member (acting as a processor) is notified by the customer of a request for erasure, rectification or restriction in relation to personal information that had been previously disclosed by a customer, the Group Member will update its records accordingly.

Confidential

Appendix 2

EU 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 led by the Vice President & Deputy General Counsel, Chief Privacy Officer (the "**CPO**"), who reports to the Executive Vice President & Chief Legal Officer who has responsibility for all legal and corporate security functions within Verizon.

1.3 The CPO oversees the US Privacy Team and the International Privacy Team. The latter covers all regions where Verizon has a presence other than the US, principally Europe, the UK, Latin America, Asia Pacific and Canada. The responsibilities of each team in the OPS and its reporting channels are clearly identified.

International

The Director, International Privacy

1.4 The Director, International Privacy is based in Verizon's International HQ in the UK, and is responsible for all aspects of privacy compliance and processing pursuant to the GDPR and applicable laws throughout Verizon's Group Members.

1.5 The International Privacy Team comprises of 4 privacy counsel based in Reading in the UK. All report to the Director, International Privacy and deal with matters of compliance outside the US. The International Privacy Team is further supported by a legal counsel and privacy specialist based in Dublin.

1.6 More specifically, the Director, International Privacy's responsibilities include:

- ensuring Verizon's compliance with Verizon's EU and UK Binding Corporate Rules Controller and Processor Policies;
- in cases where the Internal Audit Department identifies areas of non-compliance with Verizon's EU and UK Binding Corporate Rules Controller and Processor Policies, instructing the Verizon Compliance team to correct and ensuring that these are corrected within a reasonable timescale and to report accordingly to the EU Privacy Steering Committee;
- reviewing new products and services from a privacy perspective to ensure compliance with international privacy laws;
- maintaining and updating Verizon's privacy policies and privacy-related instructions;
- counselling business units on internal and external privacy principles and requirements;
- ensuring Verizon's compliance with international privacy laws, regulations, principles and policies;
- responding to regulatory bodies and industry organisations regarding opinions, proposals and drafts of proposed changes to international privacy legislation and policy;

- working with Verizon Security on security issues which relate to customer or employee privacy;
- providing face-to-face and online privacy training where employees (in teams such as Human Resources, Sales, Customer Services and Billing) are required to have a heightened awareness of international privacy issues;
- providing privacy training and updates to employees on existing and new privacy law and policies, including the EU and UK 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 international privacy law; and
- ensuring compliance with all in-country elements of international privacy law including, where necessary, ensuring that data protection registrations and notifications are complete and permits for the international transfer of personal data are obtained.

1.7 The Director, International Privacy reports directly to the CPO and, in her role as Data Protection Officer, to the Executive Vice President & Chief Legal Officer. The Director, International Privacy therefore enjoys the highest management support in exercising her functions.

International Regulatory Officers

1.8 In addition to the International Privacy Team, Verizon has a team of in-country International Regulatory Officers who are responsible for data protection compliance in European countries where Verizon operates and the UK. Regulatory Officers assist the International Privacy Team and local employees with specific in-country privacy issues and are a conduit for communication between the International Privacy Team and local competent supervisory authorities where required.

EU Privacy Steering Committee

1.9 The EU Privacy Steering Committee of Verizon Ireland Limited, is chaired by one of the directors of Verizon Ireland Limited and made up of personnel both from Verizon Ireland Limited and Verizon more broadly with expertise relevant to data processing activities under the EU Binding Corporate Rules Controller and Processor Policies ("**EU BCR Policies**"). The participants include representatives from Legal, Compliance, Policy, HR and Security as well as the Director, International Privacy.

1.10 The EU Privacy Steering Committee forms an integral part of the OPS and covers the following areas:

- implementation and monitoring of the EU BCR Policies compliance programme throughout Verizon;
- setting parameters for the annual audit of EU BCR Policies compliance, instructing auditors and implementing recommendations arising from the annual audit. Verizon Ireland Limited, with assistance from the EU Privacy Steering Committee, is the instructing party for the annual audit and will oversee the implementation of recommendations arising from the annual audits that will be carried out within Group Members in relation to the EU BCR Policies;
- making the annual EU BCR Policies update to the lead supervisory authority in relation to the EU BCR Policies;

- monitoring the process for the accession of new Group Members to the EU BCR Policies;
- the review and approval of policies and procedures to give effect to the EU BCR Policies;
- receiving regular reports on data protection matters from Verizon's Director, International Privacy, the Compliance Team and others as appropriate;
- making recommendations or approving plans put forward by the relevant Verizon teams reporting to the Committee;
- issuing quarterly reports (in the form of minutes of meetings) on the work of the Committee undertaken in relation to the EU BCR Policies; and
- working with and providing input as required to the legal team in relation to any claims under the EU BCR Policies in respect of which Verizon Ireland Limited accepts liability.

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

1.11 The Verizon US Privacy Team serves as a centralised privacy and compliance function within the US. The US Privacy Team also provides support to the Chief Information Security Officer and the International Privacy Team when appropriate on matters that cross multiple regions.

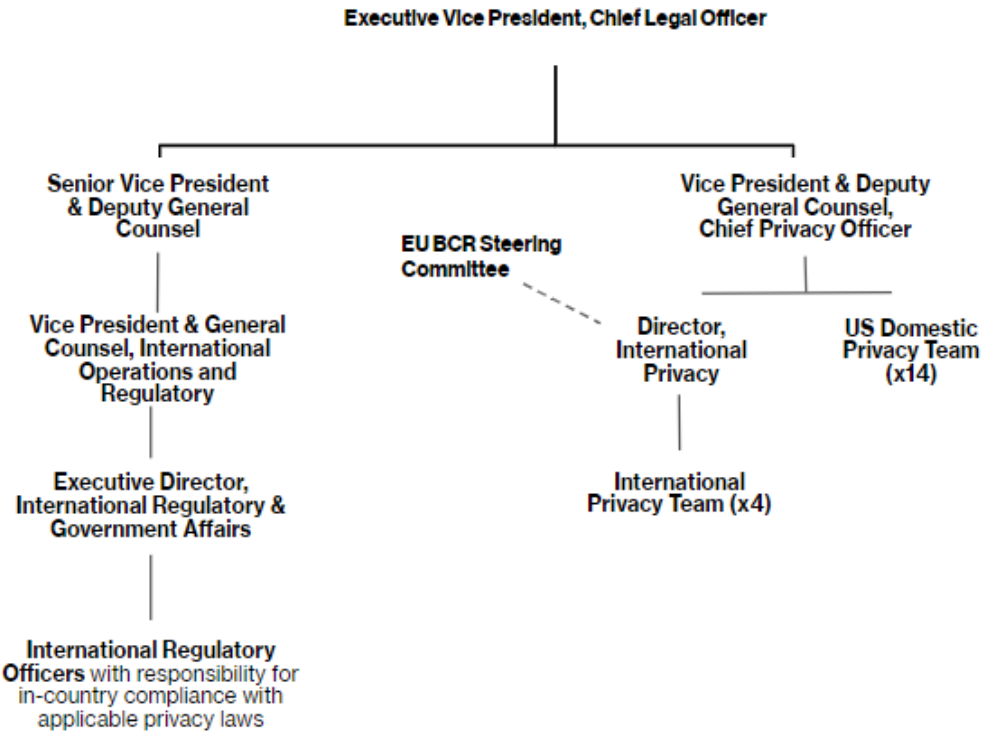
1.12 The Verizon US Privacy Team is responsible for:

- 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.

1.13 In addition to the functions described above, the CPO sits on the company's Compliance Council and the Executive Security Council (VESC). The CPO also reports to the Audit Committee of the Board of Directors and regularly meets with Verizon's Internal Audit team.

Confidential

Annex 1 – Verizon Organisational Privacy Structure



Appendix 3

Privacy Training Requirements

1. **BACKGROUND**

1.1 The purpose of this Privacy Training Requirements document is to provide a summary of how Group Members train their staff (the "**employees**") on the requirements of the EU and UK Binding Corporate Rules Controller and Processor Policies (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, International Privacy, 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, or who are involved in the processing of personal information or in the development of tools to process personal information, receive additional tailored training on international privacy principles, including on the Policies (the "**International Privacy 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 International Privacy training are together referred to in this document as the "**Privacy and compliance training program**".

2. **OVERVIEW OF TRAINING**

2.1 All Group Members' employees are required to participate in the General Privacy training program once every two years. The program is called "*Privacy and Information Security*" and alternates 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.

2.2.1 In addition to the yearly training described in section 2.1 and 2.2, where relevant to an employee's role, training will cover the following procedures under the Policies.

(a) Individuals' Rights Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure.

Confidential

3. AIMS OF THE PRIVACY AND COMPLIANCE TRAINING PROGRAM

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 with permanent or regular access to personal information, or who are involved in the processing 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 International Privacy 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, privacy and security; 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. 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.

Confidential

Appendix 4

EU Audit Protocol

1. **BACKGROUND**

1.1 Group Members are required to audit their compliance with the EU Binding Corporate Rules Controller Policy ("**EU Controller Policy**") and the EU Binding Corporate Rules Processor Policy ("**EU Processor Policy**") (together the "**Policies**") and satisfy certain conditions in so doing, and this document describes how Group Members deal with such requirements.

1.2 The role of Verizon's Director, International Privacy in the International headquarters in the UK and the network of Regulatory Officers is to provide guidance about the processing of personal information subject to the Policies and to assess the processing of personal information by Group Members for potential privacy-related risks. The processing 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 Group Members to ensure compliance with the Policies as required by the competent supervisory authorities, this is only one way in which Group Members ensure that the provisions of the Policies 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, International Privacy.

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, International Privacy and that any corrective actions to ensure compliance take place within a reasonable timescale.

2.1.3 To the extent that a Group Member acts as a processor, audits of compliance with the commitments made in the EU Processor Policy may also be carried out by or on behalf of Verizon's customers in accordance with the terms of any contract Verizon has with a customer 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. 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 Policies will take place:

(a) annually in accordance with the Group Members' audit procedure(s); and/or

(b) more frequently, at the request of Verizon Ireland Limited.

2.2.2 To the extent that a Group Member processes personal information on behalf of a third party controller, audit of the EU Processor Policy , including inspections conducted by the third party controller or by independent, accredited auditors selected by that controller, will take place as required under the contract in place between that Group Member and that third party controller.

2.2.3 The scope and coverage 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; the nature, method and location of the personal information processed; IT systems, applications and databases; onward transfers; and issues arising from conflict of laws or vendor management.

2.2.4 In the event that a third party controller on whose behalf a Group Member processes personal information exercises its right to audit the Group Member for compliance with the EU 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. Group Members 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 Group Members may use other accredited internal/external auditors as determined by the Group Members.

2.3.2 In the event that a third party controller on whose behalf a Group Member processes personal information exercises their right to audit the Group Member for compliance with the EU 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, where applicable, in agreement with the competent supervisory authority.

2.4 Report

2.4.1 On completion of the audit, the report and findings will be made available to the EU Privacy Steering Committee, the Director, International Privacy and the Executive Director, Legal & Regulatory Affairs Europe. 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. Where appropriate, the result may be communicated to the board of the ultimate parent of Verizon Communications, Inc.

2.4.2 Upon request, Group Members have agreed to:

(a) provide copies of the results of any audit of the Policies to any competent supervisory authority who will upon receiving the audit results be reminded of their duty of professional secrecy under Article 54(2) GDPR; and

(b) to the extent that an audit performed under section 2.2.2 above relates to personal information processed by Group Members on behalf of a third party controller, to make the results of any audit of compliance with the EU Processor Policy available to that controller.

2.4.3 Verizon's Director, International Privacy will be responsible for liaising with the competent supervisory authorities for the purpose of providing the information outlined in section 2.4.2(a).

Confidential

2.4.4 In addition, all Group Members agree to be audited by competent supervisory authorities in accordance with applicable audit procedures of such competent supervisory authorities, who will be reminded of their duty of professional secrecy under Article 54(2) GDPR.

Confidential

Appendix 5

EU Complaint Handling Procedure

1. Introduction

1.1 The purpose of this EU Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Group Members under the EU Binding Corporate Rules Controller Policy ("**EU Controller Policy**") and the EU Binding Corporate Rules Processor Policy ("**EU Processor Policy**") (together the "**Policies**") are dealt with.

2. **HOW INDIVIDUALS CAN BRING COMPLAINTS**

2.1 All complaints made under the Policies whether a Group Member is processing information on its own behalf or on behalf of a customer can be brought in writing to Verizon's Director, International Privacy at emeadataprotection@verizon.com, or by writing to Director, International Privacy, Verizon, 2nd Floor Boru House Block T, East Point Business Park, Dublin DO3 R6C6, Republic of Ireland.

3. **WHO HANDLES COMPLAINTS?**

3.1 *Complaints where a Group Member is a controller*

3.1.1 Verizon's Director, International Privacy will handle all complaints arising under the EU Controller Policy in respect of the processing of personal information where a Group Member is the controller of that information. Verizon's Director, International Privacy will liaise with relevant business units to investigate the complaint. The Director, International Privacy will coordinate a response.

3.1.2 What is the response time?

Verizon's Director, International Privacy 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 and number of requests, a substantive response cannot be given within this period, Verizon's Director, International Privacy will advise the complainant of the reason for the delay within one month of receipt of the complaint, and provide a reasonable estimate (not exceeding two further months from the date on which the individual was notified of the extension) 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, International Privacy (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 Vice President & Deputy General Counsel – Chief Privacy Officer ("**CPO**") 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 CPO will respond to the complainant within one month of the referral. If, due to the complexity of the complaint and number of requests, a substantive response cannot be given within this period, the CPO will advise the complainant of the reason for the delay within one month of receipt of the referral, and provide a reasonable estimate for the timescale (not exceeding two further months) within which a response will be provided. If the complaint is upheld, the CPO will arrange for any necessary steps to be taken as a consequence.

3.1.4 Individuals whose personal information is processed under the EU Controller Policy also have the right to: i) complain to a competent supervisory authority in the Member State in which the alleged infringement took place, or in which the individual works or habitually resides; ii) and/or to bring proceedings in the courts of a Member State, as described in Section C of the EU Controller Policy. These rights will apply whether or not they have first made a complaint to Verizon.

3.2 *Complaints where a Group Member is a processor*

3.2.1 Where a complaint arises under the EU Processor Policy in respect of the processing of personal information where a Group Member is the processor in respect of that information, the Group Member 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 processed and transferred between Group Members on behalf of that customer under the EU Processor Policy have the right to complain to Verizon and Verizon will deal with such complaints in accordance with this Complaint Handling Procedure. In such cases, individuals also have the right to complain to a competent supervisory authority in the Member State in which the alleged infringement took place, or in which the individual works or habitually resides; and/or to bring proceedings in the courts of a Member State as described in Section C of the EU Processor Policy and this will apply whether or not they have first made a complaint to Verizon.

Confidential

Appendix 6

EU Co-operation Procedure

1. **INTRODUCTION**

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

2. **CO-OPERATION PROCEDURE**

2.1 Where required, Verizon will make the necessary personnel available for dialogue with a supervisory authority in relation to the Policies.

2.2 Verizon will actively review and consider:

(a) any decisions made by competent supervisory authorities on any data protection law issues that may affect the Policies; and

(b) the views of the European Data Protection Board and any successor body as outlined in its published EU guidance on Binding Corporate Rules for controllers and processors.

2.3 Upon request, Verizon will provide copies of the results of any audit of the Policies to any competent supervisory authority who will upon receiving the audit results be reminded of their duty of professional secrecy under Article 54(2) GDPR.

2.4 Where any Verizon group member acts as a controller ("**Controller Group Member**") Verizon agrees that:

2.4.1 where the Controller Group Member is located within the jurisdiction of a competent supervisory authority based in Europe, that particular competent supervisory authority may audit that Controller Group Member for the purpose of reviewing compliance with the EU Controller Policy; and

2.4.2 in the case of a Controller Group Member located outside Europe, that a competent supervisory authority based in Europe may audit that Controller Group Member for the purpose of reviewing compliance with the EU Controller Policy;

in each case in accordance with applicable audit procedures of such competent supervisory authorities, who will be reminded of their duty of professional secrecy under Article 54(2) GDPR.

2.5 Where any Group Member is acting as a processor under the EU Processor Policy, that Group Member will cooperate with and accept to be audited by the competent supervisory authority competent for the relevant controller with full respect of the applicable audit procedures of such competent supervisory authorities, who will be reminded of their duty of professional secrecy under Article 54(2) GDPR.

2.6 Verizon agrees to abide by a formal advice of the competent supervisory authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

Confidential

Appendix 7

EU Updating Procedure

1. **INTRODUCTION**

1.1 This EU Updating Procedure sets out the way in which Verizon will communicate changes to the EU Binding Corporate Rules Controller Policy ("**EU Controller Policy**") and to the EU Binding Corporate Rules Processor Policy ("**EU Processor Policy**") (together the "**Policies**") to the competent supervisory authorities, individuals, its customers and to the **Group Members** bound by the Policies.

2. **MATERIAL CHANGES TO THE POLICIES**

2.1 Verizon will communicate any material changes to the Policies without undue delay to the supervisory authority acting as lead supervisory authority (the "**BCR Lead**") and, via the BCR Lead, to any other supervisory authorities concerned.

2.2 Where a change to the EU 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 European data protection law, through any legislative, court or supervisory authority measure to the BCR Lead and via the BCR Lead to any other supervisory authorities concerned at least once a year. Verizon will also provide a brief explanation to the BCR Lead and via the BCR Lead to any other supervisory authorities concerned of the reasons for any notified changes to the Policies.

3.2 Verizon will make available changes to the EU 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 European data protection law, through any legislative, court or competent 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, International Privacy 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 individuals who benefit from the Policies, via the Verizon website https://www.verizon.com/about/privacy/binding-corporate-rules.

4.3 Verizon's Director, International Privacy will maintain an up to date list of the changes made to the Policies, the list of Group Members bound by the Policies and, in regard to the Processor Policy, a list of the sub-processors appointed by Verizon to process personal information on behalf of its customers. The list of Group Members and any updates to the Policies will be available to and accessible by the individuals and competent supervisory authorities (and to the customer in the case of the EU Processor Policy) upon request.

5. NEW GROUP MEMBERS

5.1 Verizon's Director, International Privacy, overseen by the EU Privacy Steering Committee, will ensure that all new Group Members are effectively bound by and can deliver compliance with the Policies before a transfer of personal information to them takes place.