VERIZON BUSINESS GROUP

UK BINDING CORPORATE RULES CONTROLLER POLICY

Updated June 2023

CONTENTS

Confidential

INTRODUCTION TO THIS POLICY

This UK Binding Corporate Rules Controller 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 UK BCR Controller group members ("**Group Members**") when Processing that information for their own purposes or as a Processor on behalf of another Group Member.

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:

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information;

"**Customer**" means an individual or Third Party to which a Group Member supplies a service or product;

"**Exporting Entity**" means a Group Member established in the UK that is Processing Personal Information as a Controller and transferring such Personal Information to an Importing Entity under this Policy;

"**Employee**" means past, present and prospective full or part-time, temporary or permanent employees, staff, individual contractors, secondees and interns of a Group Member.

"**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and 2020 and its successor laws.;

"**ICO**" means the Information Commissioner;

"**Importing Entity**" means a Group Member established outside the UK receiving Personal Information directly from an Exporting Entity or via another Group Member outside the UK under this Policy;

"Local Data Protection Law" means any applicable local and national data protection law of a third country.

"**Personal Information**" means any information subject to UK Data Protection Law which relates to an identified or identifiable natural person processed by Verizon including but not limited to Employees, Customers receiving services from Verizon, suppliers (for example, vendors providing HR services on behalf of Verizon) and Customers' and suppliers' end-users (for example, personal data relating to the drivers of vehicles which contain telematics products) (each referred to as an "individual" in this Policy);

"**Processing**" means any operation that Verizon performs on Personal Information, whether manually or by automatic means. References to the "collection", "use" and "transfer" of Personal Information are all elements of the definition of Processing;

"**Processor**" means the entity which processes Personal Information on behalf of the Controller;

"**Profiling**" means any form of automated Processing consisting of the Processing of Personal Information to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"**Special Categories of Personal Information**" means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying an individual, data concerning health or data concerning a natural person's sex life or sexual orientation;

"**Third Party**" means an individual or entity which is not a Group Member or a data subject of a Group Member; and

"**UK Data Protection Law**" means the United Kingdom's Data Protection Act 2018, the GDPR and regulations made thereunder as amended from time to time.

This Policy applies to all Personal Information which is transferred from Exporting Entities to Importing Entities.

This Policy applies to all such Personal Information processed by Verizon (i) in the course of Customer and supplier management (including end-users of Verizon's products and services), and (ii) which relates to Employees.

Group Members and their Employees must comply with and respect this Policy when Processing Personal Information for their own purposes and as a Processor on behalf of another Group Member.

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?

UK Data Protection Law gives people the right to control how their Personal Information is processed. When Verizon processes the Personal Information of individuals this is covered and regulated by UK Data Protection Law.

Under UK 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. So for example, where we are an employer, we will be the Controller of the Personal Information that we process about our Employees.

When, on the other hand, an organisation processes information on behalf of another entity (for example, to provide a service), the former is deemed to be a *Processor* of the information and the latter will be primarily responsible for meeting the legal requirements.

HOW DOES DATA PROTECTION LAW AFFECT VERIZON INTERNATIONALLY?

UK Data Protection Law does not allow the transfer of Personal Information to a third country outside the UK unless: (i) the third country in question ensures an adequate level of protection; or (ii) there are appropriate safeguards in place to protect such personal data; or (iii) one or more of the derogations in the GDPR applies. Some of the countries in which Verizon operates are not considered to provide an adequate level of protection for individuals' data privacy rights under UK Data Protection Law and derogations are not applicable in many cases.

WHAT IS VERIZON DOING ABOUT IT?

To avoid breaking the law, Verizon must take proper steps to ensure that its Processing of Personal Information on an international basis is safe and, hence, lawful. The purpose of this Policy, therefore, is to set out a framework to satisfy the standards contained in UK Data Protection Law and, as a result, provide an adequate level of protection for all Personal Information which is transferred from Exporting Entities to Importing Entities.

This Policy is legally binding and applies to all Group Members and their Employees where those Group Members process Personal Information both manually and by automatic means, and requires that Group Members who process Personal Information as a Controller, or as a Processor on behalf of a Controller Group Member, comply with the Rules set out in **Part II** of this Policy (as applicable) 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 UK Binding Corporate Rules Processor Policy when they process Personal Information as a Processor for a Controller which is not a Group Member. Some Group Members may act as both a Controller/Processor for another Group Member and as a Processor for a Controller that is not a Group Member, and must therefore comply with this Policy and also the UK Binding Corporate Rules Processor Policy as appropriate.

WHAT PERSONAL INFORMATION DOES THIS POLICY COVER?

Personal Information processed under this Policy specifically relates to:

- **Customers and prospective Customers** including Customer contact names; addresses; job title, contact telephone numbers; email addresses; bank account numbers; directors' details including names, professional addresses and dates of birth; IP addresses; call detail records (CRDs); audio and images in connection with recorded calls including video calls; data collected for Customer support; username and passwords; level of responsiveness to marketing; CCTV images from Verizon premises;

- **suppliers and prospective suppliers** including company contact information including names, professional addresses and telephone numbers of company contacts; directors' information including names, professional addresses and dates of birth; audio and images in connection

with recorded calls including video calls; CCTV images from Verizon premises;

- **Employees** including name; address; date of birth; photograph; marital status; sexual orientation next of kin; contact telephone number; email address; email and IP traffic; unique identifiers of company-issued devices; audio and images in connection with recorded calls including video calls; CCTV images from Verizon premises; educational history and qualifications; results of background checks; bank account details; national identity and/or social security number; driving licence details; passport details; health information and health records; salary and bonus details; information relating to performance and conduct; pension contributions; membership of benefits schemes including private health schemes; areas of expertise and disciplinary information;

- **end-users** including name; contact information; date of birth; occupation/employment; marketing preferences; vehicle information; survey information and responses and images; IP addresses; phone numbers, call detail records (CDRs); and

- **business contacts** including name; contact information; job title; audio and images in connection with recorded calls including video calls and CCTV images from Verizon premises.

FOR WHAT PURPOSES IS PERSONAL INFORMATION TRANSFERRED UNDER THIS POLICY?

- Transfers of **Customer** Personal Information are made for the purposes of Customer management including: billing; marketing; providing, evaluating and monitoring the quality of products and services; providing training and Customer support services; IT development and security.

- Transfers of **supplier** Personal Information are made for the purposes of supplier management, including supply chain accounts and record keeping.

- Transfers of **Employee** Personal Information are made for operational purposes, including: emergency contact; compliance with mandatory reporting obligations and other regulatory requirements; investigations relating to fraud and disciplinary matters; management of workforce; diversity reporting, the operation of internal global employee contact directories; administration; the management of training; payroll and benefit administration; and recruitment and performance and talent management.

- Transfers of **end-user** Personal Information are made for the purposes of Customer and supplier management including: enabling Group Members to provide services to Customers or to benefit from the services provided to Verizon by suppliers.

- Transfers of **business contacts** Personal Information are made for the purposes of business management including: enabling visitors outside of customer/supplier relationships to attend meetings or conferences held by a Group Member.

Personal Information may be transferred from Exporting Entities to Importing Entities located in third countries which consists of Australia, Brazil, Chile, Hong Kong, India, Malaysia, Mexico, Peru, the Philippines, Singapore, Taiwan, Thailand and the United States.

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.

Confidential

Attention:	**Director, International Privacy**
Email:	**EMEAdataprotection@intl.verizon.com**
Telephone:	**+ 44 (0)118 905 5000**
Address:	**Verizon, Legal Department, Reading International Business Park, Basingstoke Road, Reading RG2 6DA**

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: CONTROLLER OBLIGATIONS

This Policy applies in all cases where a Group Member processes and transfers Personal Information as a Controller or, as applicable, as a Processor on behalf of a Controller Group Member.

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles of UK Data Protection Law that a Group Member must observe when it processes and transfers Personal Information as a Controller or, as applicable, as a Processor on behalf of a Controller Group Member.
- Section B deals with the practical commitments made by Group Members to the ICO in connection with this Policy.
- Section C describes the third party beneficiary rights that Group Members have granted to individuals under Part II of this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS AND FAIRNESS

Rule 1A – Group Members will first and foremost comply with Local Data Protection Law where it exists.

As an organisation, Group Members will always comply with any applicable legislation relating to Personal Information (e.g. in the UK, UK Data Protection Law) and will ensure that where Personal Information is processed this is done in accordance with Local Data Protection Law.

Where this Policy applies and:

- there is no law or the law does not meet the standards set out by the Rules in this Policy, Group Members' position will be to process Personal Information adhering to the Rules in this Policy;
- Local Data Protection Law requires a higher level of protection than is provided for in this Policy, the higher level of protection will take precedence over this Policy; or
- any applicable local legislation prevents Group Members from fulfilling, or has a substantial effect on its ability to comply with its obligations under this Policy, Group Members will follow the process set out in Rule 15.

Rule 1B – Group Members will ensure that its Processing of Personal Information is fair and lawful and that a legal basis exists for Processing of Personal Information, where required.

Group Members will ensure that their Processing of Personal Information is fair and lawful, and that a legal basis for Processing Personal Information exists where required. Group Members will only process that Personal Information where:

- the individual has given consent to the Processing of his or her Personal Information for one or more specific purposes and that consent meets the required standards under UK Data Protection Law; or
- it is necessary for the performance of a contract to which the individual is party, or in order to take steps at the request of the individual before entering into a contract; or
- it is necessary for compliance with a legal obligation to which the Group Member is subject where that legal obligation derives from the law of the UK; or

- it is necessary in order to protect the vital interests of the individual or of another individual, where the individual is physically or legally incapable of giving consent; or

- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Group Member where that Processing is set out under the law of the UK; or

- it is necessary for the purposes of the legitimate interests pursued by a Group Member or by a Third Party, except where those interests are overridden by the interests or fundamental rights and freedoms of the individual.

Where the Processing of Personal Information relates to criminal convictions and offences or related security measures, Group Members will not carry out such Processing otherwise than under the control of official authority or when the Processing is authorised by the law of the UK that provides appropriate safeguards for the rights and freedoms of individuals.

Rule 1C – Group Members will only process Special Categories of Personal Information where explicit consent has been obtained unless they have an alternative legal basis for Processing consistent with the applicable UK Data Protection Law.

Processing of Special Categories of Personal Information is only permitted on certain grounds, with the following being most relevant to Processing undertaken by Group Members:

- Group Member has obtained explicit consent to the Processing of any special category of Personal Information relating to that individual for one or more specified purposes unless UK Data Protection Law provides that the prohibition to Processing special category data may not be lifted by an individual; or

- the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Group Members or of the individual in the field of employment and social security and social protection law in so far as it is authorised by the law of the UK or a collective agreement pursuant to the law of the UK providing for appropriate safeguards for the fundamental rights and interests of individuals; or

- the Processing is necessary in order to protect the vital interests of a data subject or another individual where the individual is physically or legally incapable of giving consent; or

- the Processing relates to Personal Information that is manifestly made public by the individual; or

- the Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in a judicial capacity; or

- the Processing is necessary for reasons of substantial public interest on the basis of the law of the UK provided that it is proportionate to the aim pursued, respects the essence of data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the individual; or

- the Processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the Employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of the law of the UK provided that the Processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under the law of the UK or by rules established by national competent bodies; or

- the Processing is necessary for reasons of public health which provides for suitable and specific measures to safeguard the rights and freedoms of individuals, in particular duties of professional confidentiality.

Rule 1D – Group Members will assess the impact of any Processing of Personal Information that will involve high risks to the rights and freedoms of individuals.

Group Members will assess the necessity and proportionality of any new Processing of Personal Information, and in the case it involves high risks to the rights and freedoms of individuals, it will carry out a data privacy impact assessment. In the event that the data protection impact assessment indicates that the Processing will result in a high risk to individuals, Group Members will be required to consult the ICO prior to beginning Processing in the absence of measures taken to mitigate the risk.

Group Members acting as Processors on behalf of other Group Members will be required to co-operate as appropriate to assist Controllers in ensuring compliance with their obligations under this Rule 1D.

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

Rule 2A – Group Members will explain to individuals, at the time their Personal Information is collected, how that information will be processed.

Group Members will ensure that individuals are always told in a clear and comprehensive way (usually by means of a fair Processing statement) how their Personal Information will be processed. The relevant Group Member will provide the information required by UK Data Protection Law, which will include the following:

- the identity and contact details of the Controller, the data protection officer, the recipients, or classes of recipients;
- the purpose and legal basis for Processing, including an explanation about any Processing based on legitimate interests and any new or different compatible purposes;
- information about the safeguards in place to protect Personal Information when it is transferred internationally and how to obtain a copy of such safeguards. In the case of transfers of Personal Information between an Exporting Entity and an Importing Entity based on this Policy, the information provided will include reference to this Policy and how to access it;
- the length of time for which Personal Information will be retained, or the criteria applied to calculate this;
- details of individuals' rights, including right of access, rectification, erasure, restriction, objection, portability, the right to withdraw consent (where Processing is based on consent) at any time and the right to complain to the ICO;
- whether the provision of the information is a statutory or contractual requirement, as well as whether the data subject is obliged to provide the personal data and the consequences of the failure to provide Personal Information in such circumstances; and
- information about the existence of automated decision-making, including Profiling, and at least in cases where such decisions produce legal effects concerning the individual or similarly significantly affect the individual, or are based on Special Categories of Personal Information, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the individual.

This information will be provided when Personal Information is obtained by a Group Member from the individual.

Where a Group Member obtains an individual's Personal Information from a source other than that individual, the Group Member will provide this information to the individual, together with information about the source and categories of information received from third parties, as follows:

- within a reasonable period of time after Personal Information is collected, but at the latest within one month;
- if the Personal Information is to be processed for communication with the individual, at the latest at the time of the first communication to that individual; or,
- if it is to be disclosed to a Third Party, no later than the time when the data is first disclosed.

Where the Personal Information is collected from a Customer, the Group Member will be the Controller in respect of the Personal Information processed by them for Customer management purposes (e.g. billing) as explained in the section "For what purposes is Personal Information transferred under this Policy?", but in other aspects of the Processing that the Group Members carries out when providing services to Customers, the Group Members will be the data Processor. In such cases, the Group Member will, in the terms of its contracts with a Customer, contractually bind its Customer to ensure that Rule 2A is satisfied by that Customer.

Group Members will follow this Rule 2A unless not providing information is specifically permitted by UK Data Protection Law.

Rule 2B – Group Members will only process Personal Information for those purposes which are known to the individual or which are within their expectations and are relevant to the Group Member.

Rule 1A provides that Group Members will comply with any applicable legislation relating to the Processing of Personal Information. This means that Group Members will process Personal Information for specific, explicit and legitimate purposes as described in Rule 1B, and will not process that Personal Information in a way which is incompatible with those purposes.

Under Rule 2B, Group Members will identify and make known the purposes for which Personal Information will be processed (including the secondary uses and disclosures of the information) in accordance with Rule 2A.

Rule 2C – Group Members will only process Personal Information for a different or new purpose if they have a legitimate basis for doing so, consistent with UK Data Protection Law.

If Group Members collects Personal Information for a specific purpose in accordance with Rule 2A (as communicated to the individual via the relevant fair Processing statement) and as described in Rule 2B, and subsequently Group Members wishes to process Personal Information for a different or new purpose, it will not further process that information in a way incompatible with the purpose for which it was collected.

If Group Members is not satisfied that the Processing is compatible with the original Processing, the individual's consent to the new Processing may be necessary.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Group Members will keep Personal Information accurate and up to date.

In order to ensure that the Personal Information held by Group Members is accurate and up to date, Group Members actively encourage individuals to inform Group Members when their Personal Information changes. Group Members will take every reasonable step to ensure that Personal Information that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

Confidential

Rule 3B – Group Members will only keep Personal Information for as long as is necessary, for the purposes for which it is processed.

Group Members will comply with the Verizon record retention policies and procedures as revised and updated from time to time.

Rule 3C – Group Members will only process Personal Information which is adequate, relevant and limited to what is necessary for the purposes of such Processing.

Group Members will only process Personal Information that is required in order to properly fulfil its purposes.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Group Members will adhere to its IT security policies.

Group Members will implement appropriate technical and organisational measures to protect Personal Information against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, in particular where Processing involves transmission of Personal Information over a network, and against all other unlawful forms of Processing. To this end, Group Members will comply with the requirements in the security policies in place within Verizon, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. Group Members will implement and comply with breach notification policies as required by UK Data Protection Law as described in the following Rule.

Rule 4B – Group Members will adhere to its data breach notification policy.

Group Members will adhere to Verizon's data breach notification policy (as revised and updated from time to time) which sets out the process which must be followed in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed (a "**Data Protection Breach**").

In particular, in the event of 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**"), which will analyse the details of the Data Protection Breach and notify, without undue delay:

- Verizon UK Limited; and
- where feasible, not later than 72 hours after having become aware of the Data Protection Breach, the ICO, unless the Data Protection Breach is unlikely to result in a risk to the rights and freedoms of individual.

Individuals will be notified without undue delay in cases where the Data Protection Breach is likely to result in a high risk to their rights and freedoms unless such notification is not required under UK Data Protection Law.

Data Protection Breaches suffered by Group Members, comprising 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 ICO on request.

Rule 4C – Group Members will ensure that providers of services to Group Members also adopt appropriate and equivalent security measures.

UK Data Protection Law expressly requires that where a provider of a service (acting as a Processor) to any of the Group Members has access to individuals' Personal Information (e.g. a payroll provider), Group Members must adhere to its due diligence process for the selection of the service provider and must impose strict contractual obligations evidenced in writing dealing with the security of that information and other requirements in line with UK Data Protection Law to ensure that such service providers act only on Group Members' instructions when Processing that information, and that they have in place appropriate technical and organisational security measures to safeguard Personal Information.

Rule 4D – Where one Group Member provides a service as a Processor to a Controller Group Member, the Group Members will put in place appropriate contractual provisions and security measures as required by UK Data Protection Law.

Where a Group Member (Entity A) processes Personal Information as a Processor on behalf of a Group Member Processing Personal Information as a Controller (Entity B), Entity A will:

- act only on the documented instructions of Entity B as may be set out in Appendix 8; and
- comply with the obligations set out in Part 2 of the Processing Schedule or, as appropriate, a contract or legal act entered into between Entity A and Entity B in relation to such Processing which is consistent with UK Data Protection Law in so far as it relates to the engagement of a Processor.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – Group Members will adhere to the Individuals' Rights Procedure when dealing with any queries or access requests made by individuals in connection with their Personal Information.

On request, individuals whose Personal Information is processed under this Policy, are entitled (by making a request to the relevant Group Member in accordance with the Individuals' Rights Procedure at Appendix 1) to be supplied with a copy of Personal Information held about them (including information held in both electronic and paper records), together with certain other details such as their rights in relation to their Personal Information. This is known as a subject access request in UK Data Protection Law. Group Members will follow the steps set out in the Individuals' Rights Procedure when dealing with such requests from individuals for access to their Personal Information.

Rule 5B – Group Members will deal with requests to rectify, erase, restrict, port or complete Personal Information, or objections to the Processing of Personal Information in accordance with the Individuals' Rights Procedure.

On request, individuals, whose Personal Information is processed under this Policy, are entitled to:

- request rectification, completion, erasure, or restriction, as appropriate, of their Personal Information;
- exercise their right to data portability in relation to their Personal Information; and/or
- object to the Processing of their Personal Information, including Processing for direct marketing purposes and Profiling to the extent that it is related to such marketing, as described in Rule 7.

Group Members will follow the steps set out in the Individuals' Rights Procedure when dealing with such requests.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSFERS AND ONWARD TRANSFERS

Rule 6 – Group Members will not transfer Personal Information to third parties outside the UK without ensuring adequate protection for the information in accordance with the standards set out by this Policy and in accordance with UK Data Protection Law.

In principle, transfers and onward transfers of Personal Information from Group Members in the UK to third parties outside the UK are not allowed without appropriate steps being taken as required by UK Data Protection Law. These steps may include:

- confirming that the Third Party is located in a country which the Secretary of State has found to offer an adequate level of protection for the Personal Information transferred; or
- signing up to appropriate contractual clauses; or
- ensuring that the transfer is necessary for: (i) the performance of a contract between the individual and the transferring Group Member or for the implementation of pre-contractual measures taken at the individual's request; (ii) the conclusion or performance of a contract concluded in the interest of the individual between the transferring Group Member and another party; (iii) important reasons of public interest as laid down by the law of the UK; (iv) the establishment, exercise or defence of legal claims; (v) the protection of the vital interests of the individual or other persons, where the individual to whom the Personal Information relates is incapable of giving consent; or (vi) obtaining the explicit consent of individuals, after those individuals have been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards.

RULE 7 – LEGITIMISING DIRECT MARKETING

Rule 7 – Group Members will allow individuals to opt out of receiving marketing information.

All individuals have the data protection right to object, free of charge, to the Processing of their Personal Information for direct marketing purposes. This includes the right to object to Profiling to the extent that it is related to such marketing. Group Members will honour all such opt out requests.

RULE 8 – AUTOMATED INDIVIDUAL DECISIONS

Rule 8 – Group Members will respect the right of individuals not to be subject to a decision made as a result of Processing Personal Information by automated means (including Profiling) which has a legal or similarly significant effect on them, unless the Processing is permitted under UK Data Protection Law and Group Members have put in place necessary measures to protect the legitimate interests of individuals.

There are particular requirements in place under UK Data Protection Law to ensure that no evaluation of or decision about an individual which significantly affects them can be based solely on the automated Processing of Personal Information. The exceptions to this are where:

- the Processing is authorised under UK Data Protection Law;
- the decision is necessary for entering into a contract between the individual and Group Members; or
- the individual has given their explicit consent,

Verizon does not carry out automated individuals decisions, but if it does so in the future Group Memberswill put in place measures to protect the rights and freedoms and legitimate interests of individuals such as the right for an individual to obtain human intervention in the decision, to express his or her point of view, and to contest the decision.

Confidential

SECTION B: PRACTICAL COMMITMENTS

RULE 9 – COMPLIANCE AND ACCOUNTABILITY

Rule 9A – Group Members will be responsible for and able to demonstrate compliance with this Policy and Group Members will have appropriate staff and support to ensure and oversee compliance with this Policy throughout the business.

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 9B – Group Members **will implement appropriate technical and organisational measures to enable and facilitate compliance with the Policy in practice.**

Taking into account the state of the art and cost of implementation and the scope, nature, context and purposes of the Processing, Group Members will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by UK Data Protection Law. Group Members will integrate such measures into the Processing when determining the means of the Processing, and the time of Processing itself to facilitate the protection of Personal Information being processed, and in order to ensure that, by default, only Personal Information which is necessary for each specific purpose of the Processing is processed.

Rule 9C – Group Members Processing Personal Information will maintain a written (including in electronic form) record of their Processing activities and make that record available to the ICO on request.

The data Processing records maintained by Group Members will contain:

- the Group Member's name and contact details;
- the purposes for which Personal Information is processed;
- a description of the categories of individuals about whom Personal Information is processed and the Personal Information processed;
- the categories of recipients to whom Personal Information has been or will be disclosed including recipients in third countries or international organisations;
- details of the third country or countries to which 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;
- where possible, the period for which Personal Information will be retained; and
- where possible, a general description of the technical and organisational security measures used to protect Personal Information.

RULE 10 – TRAINING

Rule 10 – Group Members will provide appropriate training to employees who have permanent or regular access to Personal Information, who are involved in the Processing 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 11 – AUDIT

Rule 11 – Group Members will comply with the Audit Protocol set out in Appendix 4.

RULE 12– COMPLAINT HANDLING

Rule 12 – Group Members will comply with the Complaint Handling Procedure set out in Appendix 5.

RULE 13 – COOPERATION WITH THE ICO

Rule 13 – Group Members will comply with the Co-operation Procedure set out in Appendix 6.

RULE 14 – UPDATE OF THE POLICY

Rule 14 – Group Members will comply with the Updating Procedure set out in Appendix 7.

RULE 15 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 15A – Group Members will ensure that where it believes that any legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on the guarantees provided by the Policy, Group Members will promptly inform Verizon UK Limited, the Director, International Privacy unless otherwise prohibited by law or a law enforcement authority.

Rule 15B – Group Members will ensure that where there is any legal requirement that a Group Member is subject to which is likely to have a substantial effect on the guarantees provided by the Policy, the Director, International Privacy will make a responsible decision on the action to take and will report to and consult the ICO.

Rule 15C – Importing Entities will ensure that, where they receive a legally binding request from a law enforcement agency or state security body for disclosure of Personal Information transferred from the UK to a country outside the UK under this Policy, they will, unless prohibited from doing so by the requesting authority, put the request on hold and promptly notify the Exporting Entity and the ICO.

Where Importing Entities receive a legally binding request for disclosure of information transferred from the UK to a country outside the UK under this Policy and are prohibited by a law enforcement authority from putting the request on hold and/or from notifying the ICO, Importing Entities will:

- use their best efforts to obtain a waiver of this prohibition in order to communicate as much information as they can as soon as possible to the ICO including information about the data requested, the requesting body and the legal basis for disclosure; and
- demonstrate to the ICO the steps they followed to deal with the request in accordance with this Policy.

If the Group Member is not able to obtain a waiver of the prohibition to notify the ICO, the Group Member will provide to the ICO 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 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.

Where the Processing is carried out by a Group Member as a Processor Processing Personal Information on behalf of a Controller Group Member, the Processor shall, in the event that Rule 15 A, B, and/or C applies to the Processing, also notify the Controller Group Member without undue delay.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

C.1 UK Data Protection Law states that individuals whose Personal Information is processed in in the UK by an Exporting Entity and transferred to an Importing Entity must be able to benefit from certain rights as third party beneficiaries, in accordance with The Contract (Rights of Third Parties) Act 1999, to enforce compliance with:

- Rules 1A to 1C of the Policy (regarding fairness, lawfulness and Processing special categories of personal data);
- Rule 2 of the Policy (regarding transparency and purpose limitation);
- Rule 3 of the Policy (regarding data minimisation and accuracy and limited storage periods);
- Rule 4 of the Policy (regarding the security of Personal Information);
- Rule 5 of the Policy (regarding individuals' rights in relation to their Personal Information);
- Rule 6 of the Policy (regarding transfers and onward transfers);
- Rule 7 of the Policy (regarding the right to opt out of direct marketing);
- Rule 8 of the Policy (regarding individuals' rights in relation to automated individual decisions);
- Rule 9B of the Policy (regarding privacy by design and by default);
- Rule 12 of the Policy (regarding complaint handling);
- Rule 13 of the Policy (regarding co-operation with the ICO);
- Rule 15 of the Policy (regarding action where national legislation prevents compliance with the Policy);
- The provisions in C1 to C4 granting third-party beneficiary rights and setting the liability and jurisdiction rules under the Policy; and
- The right to access the Policy via https://www.verizon.com/about/privacy/BCRparticipants, or to obtain a hard copy of the Policy as well as a list of the Group Members bound by this Policy,

by:

- *making a complaint*: individuals may make complaints to a Group Member (in accordance with the Complaint Handling Procedure set out in Appendix 5) and to the ICO; and/or

- *bringing proceedings*: individuals can bring proceedings against Verizon UK Limited in the courts of the United Kingdom.

C.2 These individuals may also seek appropriate redress from Verizon UK Limited, which agrees to take the necessary action to remedy any breach of the provisions listed in sub- section 1 of this Section C by any Importing Entity and, where appropriate, receive compensation from Verizon UK Limited for any damage whether material or non-material suffered by individuals as a result of a breach of the provisions listed in sub- section 1 of this Section C by an Importing Entity.

C.3 For the avoidance of doubt, individuals shall benefit from the third party beneficiary rights as described in this Section C and the courts of the United Kingdom or the ICO shall have jurisdiction as if the breach of the provisions described in this Section C or any of them was caused by Verizon UK Limited in the UK.

C.4 In the event of a claim being made in which an individual has suffered damage where that individual can demonstrate that it is likely that the damage has occurred because a breach of this Policy, Group Members have agreed that the burden of proof to show that an Importing Entity is not responsible for the breach, or that no such breach took place, will rest with Verizon UK Limited.

PART III: APPENDICES

Confidential

Appendix 1

UK 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 UK 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 UK 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 UK 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 protection for data subjects 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/international/privacy/data-subject-rights, by email to emeadataprotection@verizon.com or orally. Where an oral request is made, Verizon will document the request and provide a copy to the individual making the request before dealing with it.

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 the UK;

(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 the ICO;

(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 the UK to a country outside the UK;

(vii) the existence of any decision-making undertaken by automated means, including Profiling, and at least in those cases, meaningful information about the logic involved in as well as the significance and consequences of such Processing;

(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 Group Member outside the UK, 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 UK Group Member and relates to the Processing of Personal Information by that Group Member, if:

(i) the refusal is consistent with UK Data Protection Law; or

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

(b) where the valid request is made to a Group Member outside the UK and the Director, International Privacy is unable to deal with the request in accordance with section 3, the relevant Group Member outside the UK will only refuse the request if the grounds for such refusal are consistent with UK Data Protection Law.

4.2 The Director, International Privacy on behalf of the Group Member will within one month of the receipt of the request inform the individual of the refusal of the request, the reason for such refusal, and will also inform the individual of his/her right to complain to the ICO 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 Verizon 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 UK 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 it is the Customer's duty to handle valid requests. When necessary, the Group Member will support the Customer in fulfilling its obligations, pursuant to the following sections.

6.2 While the Group Member, as the Processor, is not responsible for the handling of valid requests according to UK Data Protection Law, an individual may attempt to communicate their valid request directly to a Group Member instead of the Customer. In such case, to the extent legally permitted and as set out in the contracts the Group Member has with its Customers, the Group Member will promptly notify Customer if the Group Member receives a valid request. 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 UK 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.

6.4 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 UK Processor Policy, have the right to raise a valid request to the Group Member and the Group Member will deal with such requests in accordance with sections 1 to 5 of this UK Individuals' Rights Procedure.

Confidential

Appendix 2

UK 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, 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, UK Data Protection Law and Local Data Protection Laws throughout Verizon's Group Members.

1.5 The International Privacy Team comprises of 4 privacy counselbased 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 UK Binding Corporate Rules Controller and Processor Policies;
- in cases where the Internal Audit Department identifies areas of non-compliance with Verizon's UK Binding Corporate Rules Controller and Processor Policies, instructing the Verizon Compliance team to correct these within a reasonable timescale;
- 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 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, the ICO and other local competent supervisory authorities where required.

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

1.9 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.

1.10 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;

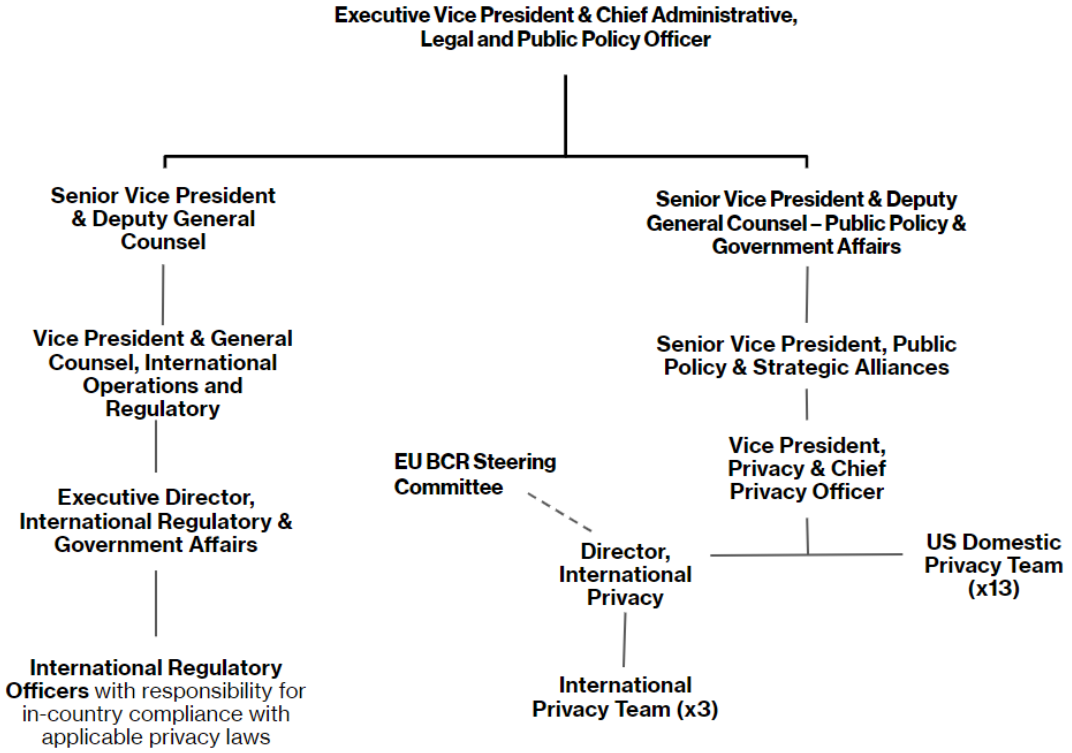
- working with Verizon Security on security issues which relate to US Customer or Employee privacy; and

- providing privacy training and updates to Employees on existing and new privacy law and policies.

1.11 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



Confidential

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 Employees on the requirements of the 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

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 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

UK Audit Protocol

1. **BACKGROUND**

1.1 Group Members are required to audit their compliance with the UK Binding Corporate Rules Controller Policy ("**UK Controller Policy**") and the UK Binding Corporate Rules Processor Policy ("**UK 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 ICO, 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 UK Processor Policy may also be carried out by or on behalf of the Group Member's Customers in accordance with the terms of the Data Processing Agreement the Group Member has with a Customer in respect of such Processing, and such audits may (at the Customer's discretion) also extend to any sub-processors acting on a Group Member'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 the Group Member and the sub-processors which includes the right for Customers of Group Members to audit 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 Member's audit procedure(s); and/or

(b) more frequently, at the request of the Director, International Privacy.

2.2.2 To the extent that a Group Member processes Personal Information on behalf of a third party ("**Third Party Controller**"), audit of the UK 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 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 UK 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 UK 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 ICO.

2.4 Report

2.4.1 On completion of the audit, the report and findings will be made available to the Director, International Privacy and the Executive Director, Legal & Regulatory Affairs Europe (also responsible for the UK). A summary of the findings will be provided to the Management Committee in the UK 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 the ICO who will upon receiving the audit results be reminded of its duty of professional secrecy under UK Data Protection Law; 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 UK Processor Policy available to that Controller.

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

2.4.4 In addition, all Group Members agree to be audited by the ICO in accordance with applicable audit procedures of the ICO, who will be reminded of its duty of professional secrecy under UK Data Protection Law.

Confidential

Appendix 5

UK Complaint Handling Procedure

1. **INTRODUCTION**

1.1 The purpose of this UK Complaint Handling Procedure is to explain how complaints brought by an individual whose Personal Information is processed by Group Members under the UK Binding Corporate Rules Controller Policy ("**UK Controller Policy**") and the UK Binding Corporate Rules Processor Policy ("**UK 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, Legal Department, Reading International Business Park, Basingstoke Road, Reading, RG2 6DA. When an oral complaint is made, the complaint shall be recorded by Verizon and verified with the individual making the complaint before taking any further action.

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 UK 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 Privacy & 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 UK Controller Policy also have the right to: i) complain to the ICO; ii) and/or to bring proceedings in the courts of the United Kingdom, as described in Section C of the UK 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 UK 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 UK 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 the ICO; and/or to bring proceedings in the courts of the United Kingdom as described in Section C of the UK Processor Policy and this will apply whether or not they have first made a complaint to Verizon.

Confidential

Appendix 6

UK Co-operation Procedure

1. **INTRODUCTION**

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

2. **CO-OPERATION PROCEDURE**

2.1 Where required, Group Members will make the necessary personnel available for dialogue with the ICO in relation to the Policies.

2.2 Group Members will actively review and consider:

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

(b) the views of the ICO as outlined in its published UK guidance on Binding Corporate Rules for Controllers and Processors.

2.3 Upon request, Group Members will provide copies of the results of any audit of the Policies to the ICO who will, upon receiving the audit results, be reminded of its duty of professional secrecy under UK Data Protection Law.

2.4 In addition, all Group Members agree to be audited by the ICO in accordance with applicable audit procedures of the ICO, who will be reminded of its duty of professional secrecy under UK Data Protection Law.

2.5 Group Members agree to abide by a formal advice of the ICO where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

2.6 Group Members will comply with any decisions and enforcement notices issued by the ICO.

Confidential

Appendix 7

UK Updating Procedure

1. **INTRODUCTION**

1.1 This UK Updating Procedure sets out the way in which Verizon will communicate changes to the UK Binding Corporate Rules Controller Policy ("**UK Controller Policy**") and to the UK Binding Corporate Rules Processor Policy ("**UK Processor Policy**") (together the "**Policies**") to the ICO, individuals, its Customers and to the Group Members.

2. **MATERIAL CHANGES TO THE POLICIES**

2.1 Verizon will communicate any material changes to the Policies such as those that potentially affect data protection compliance, are potentially detrimental to data subject rights, potentially affect the level of protection offered by the Policies or affect the binding nature of the Policies without undue delay to the ICO and all Group Members.

2.2 Where a change to the UK 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 UK Data Protection Law, through any legislative, court or measure introduced by the ICO to Group Members on a regular basis and to the ICO at least once a year. Verizon will also provide a brief explanation to the ICO of the reasons for any notified changes to the Policies.

3.2 Verizon will make available changes to the UK 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 UK Data Protection Law, through any legislative, court or measure introduced by the ICO 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 via the Verizon website https://www.verizon.com/about/privacy/binding-corporate-rules:

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,

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 UK 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 the ICO (and to the Customer in the case of the UK Processor Policy) upon request.

Confidential

5. NEW GROUP MEMBERS

5.1 Verizon's Director, International Privacy will ensure that any Verizon group entity can be effectively bound by and deliver compliance with the Policies before they are admitted as a new Group Member.

Confidential

Appendix 8

UK Processing Schedule

The Controller (as defined in Part 1 to this UK Processing Schedule ("**Part 1**")) wishes to appoint the Processor (also as defined in Part 1) to process certain Personal Information on its behalf in accordance with Rule 4D of the UK Binding Corporate Rules Controller Policy (the "**Policy**"). The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of UK Data Protection Law.

This Processing Schedule is to be read and interpreted in conjunction with the Policy.

Part 1: Processing Instructions

1.1. Name of Group Member as Controller: ……..……(the "**Controller**")

1.2. Name of Group Member as Processor: ……..……(the "**Processor**")

1.3. Purpose of the Processing carried out by the Processor: ……..……

1.4. The personal information processed will include the following categories of Personal Information:

(a) [list each category of personal information which will be processed, e.g. names, email addresses, financial information]

1.5. The individuals to whom the Personal Information relates are:

(a) [list each category of individuals, e.g. personnel]

1.6. The activities to be carried out by the Processor on behalf of the Controller will consist of:

(a) [describe services carried out by the Processor on the Controller's behalf in detail]

1.7. Duration of Processing carried out by the Processor: ……..……

Part 2: Processor's Obligations

2. The Processor shall:

2.1 ensure that personnel/contractors authorised to process the Personal Information described in Part 1 (the "**Data**") have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.2 inform the Controller: (a) if it is legally required to process the Data otherwise than as instructed by the Controller before such Processing occurs, unless the law requiring such Processing prohibits the Processor from notifying the Controller, in which case it will notify the Controller as soon as that law permits it to do so; and (b) about any instruction from the Controller which, in the Processor's opinion, infringes UK Data Protection Law;

2.3 not subcontract any Processing of the Data or otherwise disclose the Data to any Third Party except as authorised by the Third Party Controller in writing. Where sub-contracting is permitted the Processor will: (a) ensure that it has a written contract (the "**Processing Subcontract**") in place with the relevant subcontractor which imposes on the subcontractor the same obligations in respect of Processing of the Data as are imposed on the Processor under Rule 4D of the Policy and this Part 2 to the Processing Schedule ("**Part 2**"); (b) ensure that there are sufficient guarantees in place to ensure the Processing Subcontract meets the requirements of UK Data Protection Law; (c) remain fully liable to the Controller for its obligations under Rule 4D of the

Policy and this Part 2; and (d) ensure that Rule 6 of the Policy is complied with in the event that Data is subject to a trans-border transfer to a sub-contractor;

2.4 upon completion of the Processing carried out by the Processor on the Controller's behalf and at the choice of the Controller, return or delete all Data processed by the Processor and all copies of such information unless the Processor is prevented from doing so by UK law, in which case the Data will be kept confidential and will not be actively processed for any purpose; and

2.5 provide such co-operation and assistance as the Controller reasonably considers to be necessary to enable the Controller to: (a) verify the Processor's compliance with Rules 4A and 4D of the Policy and this Processing Schedule; (b) carry out prior assessments of Processing activities which are likely to result in a high risk to the rights and freedoms of individuals and any related consultations with the ICO; (c) fulfil its obligations in respect of any request by an individual to exercise their rights under the Policy, including by notifying the Controller without undue delay of any such request; and (d) investigate, mitigate and notify in accordance with Rule 4B of the Policy any Data Protection Breach involving the Data, including by notifying the Controller without undue delay of any such Data Protection Breach.