VERIZON ENTERPRISE SOLUTIONS

BINDING CORPORATE RULES CONTROLLER POLICY

CONTENTS

Confidential

INTRODUCTION TO THIS POLICY

This Binding Corporate Rules Controller Policy and its Appendices (together the "**Policy**") establish the approach taken by Verizon Enterprise Solutions (also referred to as Verizon Wireline and Verizon Business) ("**Verizon**") to the protection and management of personal information globally by Verizon 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;

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

"**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 and the Data Protection Act 2018, including subordinate legislation, in each case as amended from time to time;

"**Exporting Entity**" means a Group Member established in Europe that is processing personal information as a controller and transferring such personal information to an Importing Entity under this Policy; "**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation);

"**Importing Entity**" means a Group Member established outside Europe receiving personal information directly from an Exporting Entity or via another non-European Group Member under this Policy;

"**personal information**" means any information subject to European data protection law which relates to an identified or identifiable natural person processed by Verizon including but not limited to past, present and prospective employees and contractors, 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; and

"**supervisory authority**" means an independent public authority established in a European jurisdiction which is responsible for monitoring the application of European data protection law in order to protect the fundamental rights and freedoms of individuals in relation to processing.

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 and contractors.

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/BCRparticipants.

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. When Verizon processes the personal information of individuals this is covered and regulated by European data protection law.

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. 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?

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 are not regarded by supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

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 European 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 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 Binding Corporate Rules Processor Policy as appropriate.

WHAT PERSONAL INFORMATION DOES THIS POLICY COVER?

Personal information processed under this Policy includes:

- in relation to **customers**: customer contact names; addresses; contact telephone numbers; email addresses; bank account numbers; directors' details including names, professional addresses and dates of birth; IP addresses; data collected for customer support; username and passwords;

- in relation to **suppliers**: company contact information including names, professional addresses and telephone numbers of company contacts; directors' information including names, professional addresses and dates of birth;

- in relation to **employees and contractors**: name; address; date of birth; next of kin; contact telephone number; email address; IP addresses and unique identifiers of company-issued devices; educational history and qualifications; bank account details; national identity and/or social security number; health records (for sickness reporting purposes); salary and bonus details; performance details; pension contributions; membership of private health schemes and disciplinary information; and

- in relation to **end-users**: name; contact information; date of birth; occupation/employment; marketing preferences; vehicle information; survey information and responses and images; IP addresses, phone numbers and call records.

FOR WHAT PURPOSES IS PERSONAL INFORMATION TRANSFERRED UNDER THIS POLICY?

- Transfers of **customer** personal information are made from Exporting Entities to Importing Entities (including United States, India and Singapore) 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 from Exporting Entities to Importing Entities (including United States, India and Singapore) for the purposes of supplier management, including supply chain accounts and record keeping.

- Transfers of **employee and contractor** personal information are made from Exporting Entities to Importing Entities (including United States, India and Singapore) 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; 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 from Exporting Entities to Importing Entities (including United States, India and Singapore) 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.

FURTHER INFORMATION

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

Confidential

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

The Director, Privacy Policy & Compliance International is responsible for ensuring that changes to this Policy are notified 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.

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 European 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 Verizon to supervisory authorities in connection with this Policy.
- Section C describes the third party beneficiary rights that Verizon has granted to individuals under Part II of this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS AND FAIRNESS

Rule 1A – Verizon will first and foremost comply with local law where it exists.

As an organisation, Verizon will always comply with any applicable legislation relating to personal information (e.g. in Europe, European data protection law) and will ensure that where personal information is processed this is done in accordance with the local applicable 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, Verizon's position will be to process personal information adhering to the Rules in this Policy;
- applicable 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
- local applicable law prevents Verizon from fulfilling, or has a substantial effect on its ability to comply with its obligations under this Policy, Verizon will follow the process set out in Rule 15.

Rule 1B – Verizon 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. Taking into account any specific provisions of a particular European or Member State law, Group Members will only process that personal information where:

- the individual has given consent to the processing of his or her personal information and that consent meets the required standards under European 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 European law or the law of a European Member State; 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 either under European law or the law of a European Member State to which the Group Member is subject; 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 European or Member State law that provides appropriate safeguards for the rights and freedoms of individuals.

Rule 1C – Verizon will only process special categories of personal information where explicit consent has been obtained unless Verizon has an alternative legal basis for processing consistent with the applicable European 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 Verizon:

- Verizon 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 European 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 Verizon or of the individual in the field of employment and social security and social protection law in so far as it is authorised by European or Member State law or a collective agreement pursuant to Member State law 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 an individual or a third party 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 European or Member State law 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 European or Member State law provided that the processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under European or Member State law 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 – Verizon will assess the impact of any processing of personal information that will involve high risks to the rights and freedoms of individuals.

Verizon 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 competent supervisory authorities 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 – Verizon will explain to individuals, at the time their personal information is collected, how that information will be processed.

Verizon 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 European 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) and the right to complain to a supervisory authority;

- whether the provision of the information is a statutory or contractual requirement, 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.

The requirements of the local law where the personal information is collected will determine whether any additional information has to be provided to individuals and the timescale within which the required information must be provided.

This information will be provided when personal information is obtained by Verizon from the individual.

Where Verizon obtains an individual's personal information from a source other than that individual, Verizon 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, Verizon will be the controller in respect of the personal information processed by Verizon 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 Verizon carries out when providing services to customers, Verizon will be the data processor. In such cases, Verizon will, in the terms of its contracts with a customer, contractually bind its customer to ensure that Rule 2A is satisfied by that customer.

Verizon will follow this Rule 2A unless not providing information is specifically permitted by European data protection law.

Rule 2B – Verizon will only process personal information for those purposes which are known to the individual or which are within their expectations and are relevant to Verizon.

Rule 1A provides that Verizon will comply with any applicable legislation relating to the processing of personal information. This means that Verizon 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, Verizon 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 – Verizon will only process personal information for a different or new purpose if Verizon has a legitimate basis for doing so, consistent with the applicable European data protection law.

If Verizon 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 Verizon 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 Verizon 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 – Verizon will keep personal information accurate and up to date.

In order to ensure that the personal information held by Verizon is accurate and up to date, Verizon actively encourages individuals to inform Verizon when their personal information changes. Verizon 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.

Rule 3B – Verizon will only keep personal information for as long as is necessary for the purposes for which it is processed.

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

Rule 3C – Verizon will only process personal information which is adequate, relevant and limited to what is necessary for the purposes of such processing.

Verizon will only process personal information that is required in order to properly fulfil its purposes.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

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

Verizon 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, Verizon 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. Verizon will implement and comply with breach notification policies as required by applicable data protection law as described in the following Rule.

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

Verizon will adhere to its 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, Privacy Policy & Compliance International 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 competent supervisory authority, 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 European 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 competent supervisory authority on request.

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

European data protection law expressly requires that where a provider of a service (acting as a processor) to any of the Verizon entities has access to individuals' personal information (e.g. a payroll provider), Verizon 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 European data protection law to ensure that such service providers act only on Verizon's 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 European 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 European data protection law in so far as it relates to the engagement of a processor.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – Verizon 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 Verizon 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 European data protection law. Verizon 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 – Verizon 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.

Verizon 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 – Verizon will not transfer personal information to third parties outside Europe without ensuring adequate protection for the information in accordance with the standards set out by this Policy and in accordance with European data protection law.

In principle, transfers and onward transfers of personal information from Group Members in Europe to third parties outside Europe are not allowed without appropriate steps being taken as required by European data protection law. These steps may include:

- confirming that the third party is located in a country which the European Commission 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 European Union or Member State law; (iv) the establishment, exercise or defence of legal claims; (v) the protection of the vital interests of the individual or of another individual and where the individual 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 – Verizon 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. Verizon will honour all such opt out requests.

RULE 8 – AUTOMATED INDIVIDUAL DECISIONS

Rule 8 –Verizon 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 European data protection law and Verizon has put in place necessary measures to protect the legitimate interests of individuals.

There are particular requirements in place under European 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 European data protection law;
- the decision is necessary for entering into a contract between the individual and Verizon; or
- the individual has given their explicit consent,

Verizon does not carry out automated individuals decisions, but if it does so in the future Verizon will 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.

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 Verizon will have appropriate staff and support to ensure and oversee compliance with this Policy throughout the business.

Verizon has appointed its Director, Privacy Policy & Compliance International as the person to oversee and ensure compliance with this Policy, supported by legal and compliance officers at regional and country level who are responsible for overseeing and enabling compliance with this Policy on a day to day basis.

A summary of the roles and responsibilities of Verizon's privacy team is set out in Appendix 2.

Rule 9B – Verizon 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, Verizon will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by European data protection law. Verizon 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

competent supervisory authorities 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 – Verizon 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 – Verizon will comply with the Audit Protocol set out in Appendix 4.

RULE 12– COMPLAINT HANDLING

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

RULE 13 – COOPERATION WITH SUPERVISORY AUTHORITIES

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

RULE 14 – UPDATE OF THE RULES

Rule 14 – Verizon will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 7.

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

Rule 15A – Verizon will ensure that where it believes that the 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, Verizon will promptly inform Verizon UK Limited, the Director, Privacy Policy & Compliance International unless otherwise prohibited by law or a law enforcement authority.

Rule 15B – Verizon 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, Privacy Policy & Compliance International will make a responsible decision on the action to take and will consult the competent supervisory authority.

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 outside Europe under this Policy, Verizon will, unless prohibited from doing so by the requesting authority, put the request on hold and promptly notify the Exporting Entity and the competent supervisory authority.

Where Importing Entities 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, 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 competent supervisory authorities; and
- demonstrate to the competent supervisory authorities the steps they followed to deal with the request in accordance with this Policy.

Verizon will provide to the competent supervisory authority 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, Verizon 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 European data protection law states that individuals whose personal information is processed in Europe by an Exporting Entity and transferred to an Importing Entity must be able to benefit from certain rights as third party beneficiaries 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 supervisory authorities);
- Rule 15 of the Policy (regarding action where national legislation prevents compliance with the Policy);
- The provisions in C1 to C3 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 supervisory authority in the Member State in which the alleged infringement took place, or in which the individual works or habitually resides; and/or
- *bringing proceedings*: individuals can bring proceedings against Verizon UK Limited in the courts of a Member State in which Verizon has an establishment or in the Member State in which the individual has his habitual residence.

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 or any of them 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 or any of them listed in sub-section 1 of this Section C by an Importing Entity in accordance with the determination of a court or other competent authority.

C.3 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 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 UK Limited in the United Kingdom.

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, Verizon has 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

APPENDIX 1

INDIVIDUALS' RIGHTS PROCEDURE

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

Individuals' Rights Procedure

Confidential

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

Individuals' Rights Procedure

1. INTRODUCTION

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

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

(a) be informed by Verizon whether any personal information about them is being processed by Verizon and, if Verizon 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 Verizon deals 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 the applicable European data protection law differs from this Procedure and requires a higher level of protection for personal data, the local data protection law 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 Verizon.

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, 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 Verizon when Verizon is a controller of the personal information requested is entitled to:

(a) be informed whether Verizon 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 Verizon, 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 Verizon. 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, Privacy Policy & Compliance International immediately upon receipt indicating the date on which it was received together with any other information which may assist the Director, Privacy Policy & Compliance

International to deal with the request. Such requests can be sent to emeadataprotection@intl.verizon.com.

3.2 The Director, Privacy Policy & Compliance International will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity or any further information is required. 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 Verizon and Verizon has reasonable doubts concerning the identity of the individual, Verizon may request such information that it may reasonably require in order to confirm the identity of the individual making the request.

3.4 Verizon must deal with a valid request without undue delay and in any event within 1 month of its receipt. Verizon may extend this period, by up to two further months if necessary, taking into account the complexity and number of the requests. Where Verizon extends the period in which it will deal with a valid request, Verizon 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, Privacy Policy & Compliance International 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, Privacy Policy & Compliance International 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 supervisory authority or seek a judicial remedy in relation to the refusal.

5. VERIZON'S RESPONSE

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

5.2 The Director, Privacy Policy & Compliance International 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, Privacy Policy & Compliance International into a readily understandable format (internal codes or identification numbers used at Verizon that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Director, Privacy Policy & Compliance International which includes information required to be provided in response to 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 Verizon is the controller for that personal information, such a request must be considered and dealt with as appropriate by the Director, Privacy Policy & Compliance International. In particular:

(a) if the valid request is advising of a change or any inaccuracy in an individual's personal information, where Verizon is the controller for that personal information, such information must be rectified or updated accordingly if Verizon is satisfied that there is a legitimate basis for doing so;

(b) when, pursuant to a valid request, Verizon 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, Verizon will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records; and

(c) if the valid request made to Verizon 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, Privacy Policy & Compliance International. Where the processing

undertaken by Verizon 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, Privacy Policy & Compliance International.

6. REQUESTS MADE TO VERIZON WHERE VERIZON IS A PROCESSOR

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

APPENDIX 2

COMPLIANCE STRUCTURE

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

Compliance Structure

Confidential

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

Compliance Structure

1. Overview

1.1 Verizon's Organisational Privacy Structure (the "**OPS**") is a global network of privacy professionals. The structure of the OPS is shown on the attached diagram (Annex 1).

1.2 The OPS is led by the Vice President & Deputy General Counsel – Chief Privacy Officer (the "**CPO**"), who reports to the Senior Vice President & Deputy General Counsel – Public Policy and Government Affairs, who in turn has responsibility for Verizon's global public policy, federal legislative affairs, federal regulatory affairs, strategic alliances, national security, privacy, and corporate citizenship.

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, namely 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, Privacy Policy & Compliance, International (INTL)

1.4 The Director, Privacy Policy & Compliance (INTL) is based in Verizon's European HQ in the UK, and is responsible for all aspects of privacy compliance and processing pursuant to the General Data Protection Regulation and applicable laws throughout Verizon's Group Members.

1.5 The INTL Privacy Team comprises of 4 privacy counsel: 3 based in Reading in the UK, and 1 based in Arlington, Washington. All report to the Director, Privacy Policy & Compliance INTL and deal with matters of compliance outside the US.

1.6 More specifically, the Director, Privacy Policy & Compliance (INTL)'s responsibilities include:

- ensuring Verizon's compliance with Verizon's Binding Corporate Rules controller and processor policies;
- in cases where the Internal Audit Department identifies areas of non-compliance with Verizon's Binding Corporate Rules controller and processor policies, ensuring that these are corrected within a reasonable timescale;

- reviewing new products and services from a privacy perspective to ensure compliance with INTL privacy laws;
- maintaining and updating Verizon's INTL-specific privacy policies and privacy-related instructions;
- counselling business units on internal and external privacy principles and requirements;
- ensuring Verizon's compliance with INTL privacy laws, regulations, principles and policies;
- responding to regulatory bodies and industry organisations regarding opinions, proposals and drafts of proposed changes to INTL privacy legislation and policy;
- working with Verizon Security on security issues which relate to customer or employee privacy;
- providing face-to-face and net-conference privacy training where employees (in teams such as Human Resources, Sales, Customer Services and Billing) are required to have a heightened awareness of INTL privacy issues;
- providing privacy training and updates to employees on existing and new privacy law and policies, including the Binding Corporate Rules controller and processor policies;
- assisting the commercial legal team in contract negotiations and ensuring that Verizon's contracts reflect the requirements of INTL privacy law; and
- ensuring compliance with all in-country elements of INTL 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, Privacy Policy & Compliance (INTL) reports to the CPO.

INTL Regulatory Officers

1.8 In addition to the INTL privacy team, Verizon has a team of in-country EU Regulatory Officers who are responsible for data protection compliance in all European countries where Verizon operates. Regulatory Officers assist local employees with specific in-country privacy issues and are a conduit for communication between the INTL Privacy Team and local data protection 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 INTL Privacy Team when appropriate on matters that cross multiple regions.

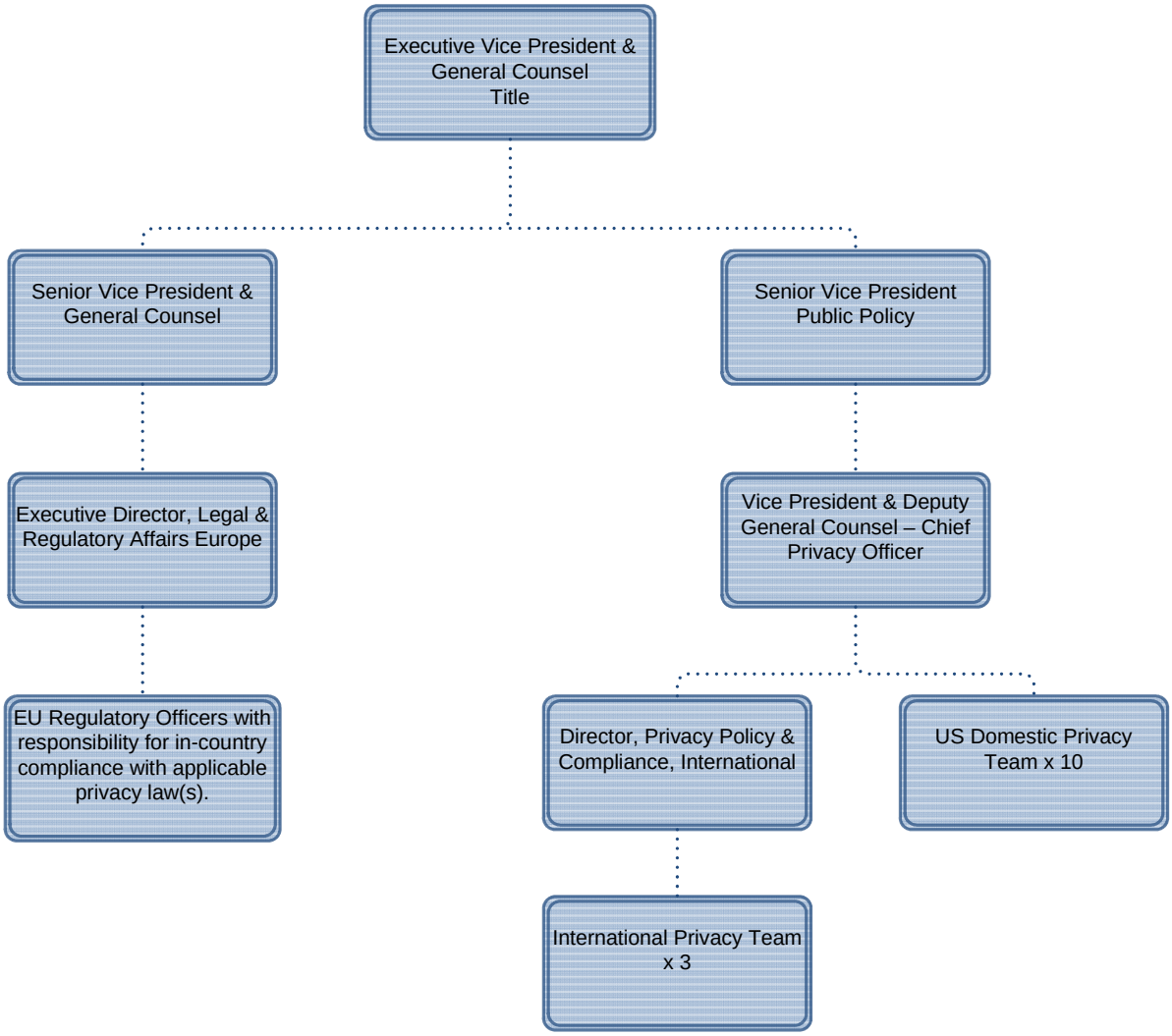
1.10 The Verizon US Privacy Team is responsible for:

- 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



APPENDIX 3

PRIVACY TRAINING REQUIREMENTS

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

Privacy Training Requirements

Confidential

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

Privacy Training Requirements

1. Background

1.1 The Controller and Processor Data Protection Binding Corporate Rules of Verizon (the "**Policies**") provide a framework for the transfer of personal information between Verizon group members ("**Group Members**"). The purpose of this Privacy Training Requirements document is to provide a summary of how Verizon trains its staff (the "**employees**") on the requirements of the Policies.

1.2 Verizon's Corporate Compliance Department has overall responsibility for compliance training within Verizon, including the delivery and tracking of Verizon's privacy training programs. Training on the Policies is overseen by the Director, Privacy Policy & Compliance International, the Chief Privacy Officer and in-region privacy professionals around the globe.

1.3 All Verizon employees receive periodic training on privacy and data protection (the "**General Privacy training**") and on Verizon's Code of Conduct. Training on other specific privacy-related matters such as Records Management, HIPAA Privacy and Security, or country-specific Data Protection is also provided on a need-to-know basis.

1.4 Employees who have permanent or regular access to personal information, 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 the Policies (the "**BCR Policies training**") and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.

1.5 The General Privacy training and the BCR Policies training are together referred to in this document as the "**Privacy and compliance training program**".

2. Overview of training at Verizon

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

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

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

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

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

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

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

3.1.3 employees in positions 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 BCR Policies training (if required) and training on Verizon's Code of Conduct shortly after joining Verizon. The Code of Conduct requires employees to follow Verizon's Privacy and Information Security policies and procedures.

3.3 General data protection and privacy training for all employees

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

3.3.2 All employees also benefit from:

(a) Code of Conduct training, which provides a detailed review of Verizon's commitment to ethical behaviour, including specific discussion of key ethics and compliance risks, 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. BCR Policies training

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

4.1.1 Background and rationale

(a) What is data protection law?

(b) How data protection law will affect Verizon internationally?

(c) The scope of the Policies

(d) Terminology and concepts

4.1.2 The Policies

(a) An explanation of the Policies

(b) Practical examples

(c) The rights that the Policies gives to individuals

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

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

(a) Individuals' Rights Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

5. Further information

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

APPENDIX 4

AUDIT PROTOCOL

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

Audit Protocol

Confidential

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

Audit Protocol

1. Background

1.1 The purpose of Verizon's Binding Corporate Rules Controller Policy and Binding Corporate Rules Processor Policy (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") is to safeguard personal information transferred between the Verizon group members ("**Group Members**").

1.2 The Policies require approval from the supervisory authorities in the European Member States from which the personal information is transferred. One of the requirements of the supervisory authorities is that Verizon audits compliance with the Policies and satisfies certain conditions in so doing, and this document describes how Verizon deals with such requirements.

1.3 The role of Verizon's Director, Privacy Policy & Compliance International in the EU headquarters in the UK and the network of Regulatory Officers is to provide guidance about the 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 Verizon to ensure compliance with the Policies as required by the supervisory authorities, this is only one way in which Verizon ensures that the provisions of the Policy are observed and corrective actions taken as required.

2. Approach

2.1 Overview of audit

2.1.1 Compliance with the Policies is overseen on a day to day basis by the Director, Privacy Policy & Compliance International.

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

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

(a) annually in accordance with Verizon's audit procedure(s); and/or

(b) more frequently, at the request of the Director, Privacy Policy & Compliance International and/or as determined necessary by the Executive Director, Legal & Regulatory Affairs in the EU.

2.2.2 To the extent that a Group Member processes personal information on behalf of a third party controller, audit of the Processor Policy will take place as required under the contract in place between that Group Member and that third party controller.

2.2.3 The scope 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 Verizon processes personal information exercises its right to audit Verizon for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, files, documents (where appropriate) and activities relating to that controller. Verizon will not provide a controller with access to systems which process personal information of other controllers.

2.3 Auditors

2.3.1 Audit of the procedures and controls in place to give effect to the commitments made in the Policies will be undertaken by Verizon’s Internal Audit Department, and Verizon may use other accredited internal/external auditors as determined by Verizon.

2.3.2 In the event that a third party controller on whose behalf Verizon processes personal information exercises their right to audit Verizon for compliance with the Processor Policy, such audit may be undertaken by that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between Verizon and that controller, where applicable, in agreement with the supervisory authority.

2.4 Report

2.4.1 On completion of the audit, the report and findings will be made available to the Director, Privacy Policy & Compliance International and the Executive Director, Legal & Regulatory Affairs Europe responsible for the EU. A summary of the findings will be provided to the EU Management Committee with details of any remedial action required, recommendations and timescales for remedial action to be undertaken. Where appropriate, the result may be communicated to the board of the ultimate parent of Verizon Communications, Inc.

2.4.2 Upon request, Verizon has agreed to:

(a) provide copies of the results of any audit of the Policies to any 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 relates to personal information processed by Verizon on behalf of a third party controller, to make the results of any audit of compliance with the Processor Policy available to that controller.

2.4.3 Verizon's Director, Privacy Policy & Compliance International will be responsible for liaising with the supervisory authorities 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 supervisory authorities in accordance with applicable audit procedures of such supervisory authorities, who will be reminded of their duty of professional secrecy under Article 54(2) GDPR.

APPENDIX 5

COMPLAINT HANDLING PROCEDURE

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

Complaint Handling Procedure

Confidential

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

Complaint Handling Procedure

1. Introduction

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

2. How individuals can bring complaints

2.1 All complaints made under the Policies whether Verizon is processing information on its own behalf or on behalf of a customer can be brought in writing or verbally to Verizon's Director, Privacy Policy & Compliance International at emeadataprotection@intl.verizon.com by telephone to 044 (0)118 905 5000, or by writing to Director, Privacy Policy & Compliance International, Verizon, Legal Department, Reading International Business Park, Basingstoke Road, Reading, RG2 6DA. Complaints made verbally 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 Verizon is a controller*

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

3.1.2 What is the response time?

Verizon's Director, Privacy Policy & Compliance International will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. If, due to the complexity of the complaint and number of requests, a substantive response cannot be given within this period, Verizon's Director, Privacy Policy & Compliance International 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, Privacy Policy & Compliance International (or the individual or department within Verizon dealing with the complaint) or any aspect of a finding, and notifies Verizon accordingly, the matter will be referred to the 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 Controller Policy also have the right to: i) complain to a 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 Controller Policy. These rights will apply whether or not they have first made a complaint to Verizon.

3.2 *Complaints where Verizon is a processor*

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

3.2.2 When a customer ceases to exist

In circumstances where a customer has disappeared, no longer exists or has become insolvent, individuals whose personal information is processed and transferred between Group Members on behalf of that customer under the Processor Policy have the right to complain to Verizon and Verizon will deal with such complaints in accordance with section 3.1 of this Complaint Handling Procedure. In such cases, individuals also have the right to complain to a 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 Processor Policy and this will apply whether or not they have first made a complaint to Verizon.

APPENDIX 6

CO-OPERATION PROCEDURE

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

Co-operation Procedure

Confidential

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

Co-operation Procedure

1. Introduction

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

2. Co-operation Procedure

2.1 Where required, Verizon will make the necessary personnel available for dialogue with a 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 guidance on Binding Corporate Rules for controllers and Binding Corporate Rules for processors.

2.3 Upon request, Verizon will provide copies of the results of any audit of the Policies to any 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 supervisory authority based in Europe, that particular supervisory authority may audit that Controller Group Member for the purpose of reviewing compliance with the Binding Corporate Rules Controller Policy; and

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

in each case in accordance with applicable audit procedures of such 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 Binding Corporate Rules Processor Policy, that Group Member will cooperate with and accept to be audited by the supervisory authority competent for the relevant controller with full respect of the applicable audit procedures of such 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 applicable supervisory authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

APPENDIX 7

UPDATING PROCEDURE

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

Updating Procedure

Confidential

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

Updating Procedure

1. Introduction

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

2. Material changes to the Policies

2.1 Verizon will communicate any material changes to the Policies 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 Processor Policy affects the conditions under which Verizon processes personal information on behalf of any customer, Verizon will also communicate such information to any affected customer before it is implemented, and with sufficient notice to enable affected customers to object. Verizon's customer may then suspend the transfer of personal information to Verizon and/or terminate the contract, in accordance with the terms of its contract with Verizon.

3. Administrative changes to the Policies

3.1 Verizon will communicate changes to the Policies which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure to the 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 Processor Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure to any customer on whose behalf Verizon processes personal information.

4. Communicating and logging changes to the Policies

4.1 The Policies contain a change log which sets out the date of revisions to the Policies and the details of any revisions made. Verizon's Director, Privacy Policy & Compliance International will maintain an up to date list of the changes made to the Policies.

4.2 Verizon will communicate all changes to the Policies, whether administrative or material in nature:

4.2.1 to the Group Members bound by the Policies; and

4.2.2 systematically to customers on whose behalf Verizon processes personal information, and to the individuals who benefit from the Policies, via the Verizon website https://www.verizon.com/about/privacy/binding-corporate-rules.

4.3 Verizon's Director, Privacy Policy & Compliance International will maintain an up to date list of the changes made to the Policies, the list of Group Members bound by the Policies and, 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 supervisory authorities (and to the customer in the case of the Processor Policy) upon request.

5. New Group Members

5.1 Verizon's Director, Privacy Policy & Compliance International 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.

APPENDIX 8

PROCESSING SCHEDULE

Confidential

Binding Corporate Rules Controller of Verizon Enterprise Solutions

Processing Schedule

Confidential

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

Processing Schedule

The Controller (as defined in Part 1 to this 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. The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of the GDPR.

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 applicable 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 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 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 Article 28 of the GDPR; (c) remain fully liable to the Controller for its obligations under Rule 4D 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 European or Member State law to which the Processor is subject, 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 competent supervisory authorities; (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.