NortonLifeLock Controller Binding Corporate Rules ("BCR-Cs")

Glossary

Audit, Audit Plan, Audit Report	**Audit** means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. **Audit Plan** is the plan which, based on the result of the risk assessment, defines the scope, objectives, and strategies of the audit. It establishes a balance between scope, timeframes, and staff days to ensure optimum use of resources. **Audit Report** is the report that documents audit findings to the Board of Directors and other internal and external recipients. It helps management evaluate NortonLifeLock's performance in protecting Personal Data and privacy and identify methods for correcting or improving adverse conditions.
Complaint	Means an expression of dissatisfaction made to NortonLifeLock related to its handling of the complainant's Personal Data, requiring a response or resolution.
Consumer	A natural person who has purchased any products or services proposed by NortonLifeLock as part of its consumer product line.
Cyber Criminal/Victim	An individual who is engaged in or threatens to engage in cyber-threatening activities which could put network and information security at risk and who may be identifiable based on network information such as IP addresses and email addresses. By extension, the term Cyber Criminal in these BCR-Cs may also refer to other originators of cyber threats and other perpetrators of cyber-attacks, even if they do not fall under the definitions of the Council of Europe's Budapest Convention on Cybercrime. Cyber Victim is an individual hit, targeted or otherwise threatened by a Cyber Criminal.
Data Controller	The entity that determines the purposes and means of Processing Personal Data.
Data Processor	The entity that Processes Personal Data on behalf of a Data Controller or other third-party entity such as another Data Processor.
Data Protection Authority	An authority appointed by an EEA Member State to implement and enforce data protection law in that State.
Data Protection Laws	The GDPR and all laws enacted in EU member states that implement requirements of the GDPR and/or give effect to derogations permitted by the GDPR and any other Data Protection Laws and regulations relating to the Processing of Personal Data and privacy (to include any relevant amendments, transpositions, successors or replacements to those laws), including where applicable, binding EU and national guidance.
DPO	Data Protection Officer. Pembroke Privacy acts as NortonLifeLock's DPO.

Data Subject	An identified or identifiable natural person whose Personal Data we may process which can include a Consumer, Employees, Cyber Criminal/Victim and in the case of Services Providers, their employees, agents or other representatives whose Personal Data is collected and processed by NortonLifeLock as a Data Controller, to whom Data Protection Laws apply.
EEA	The European Economic Area which contains all EU Member States and Norway, Lichtenstein, and Iceland.
Employee	A natural person working for another natural person or entity for pay. By extension, the term 'Employee' as used in relation to NortonLifeLock in these BCR-Cs includes all personnel, including consultants, temporary, posted, or delegated workforce, trainees and other human resources bound by NortonLifeLock's policies on Personal Data Protection, Personal Data Handling, and related privacy policies, procedures, and requirements such as mandatory privacy training.

General Data Protection Regulation or GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC, and any replacement or implementing legislation, directive, regulation, or instrument imposing equivalent obligations.
Global Privacy Policy	The NortonLifeLock global privacy policy which memorialises NortonLifeLock's principles of data protection and approach to achieving compliance with Data Protection Laws.
Privacy Legal	The department consisting of a team of attorneys and other privacy professionals employed by NortonLifeLock to ensure compliance with applicable privacy law.
Information	Information means all items that are created or received by any business unit at the Company in any of the following formats: (a) paper documents, forms, reports, manuals, correspondence, calendars, notes or files; (b) electronic files, such as spreadsheets, database contents, word-processing documents, PowerPoint files, voicemails or emails; (c) videotape, audio-tape, microfilm or photographs or other voice and video recordings such as, in particular, Zoom session recordings and similar materials; and (d) other types of electronically stored information. A piece of information is not always a Record.
Personal Data	Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
Processor (or any variation thereof)	An entity that performs any form of action on Personal Data, such as collection, access, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure or destruction.

Record	Record means a subset of Information that: (a) provides evidence of the Company's legal compliance, organization, business functions, policies, decisions, procedures, operations and/or internal or external transactions; or (b) reflects the Company's intent to preserve such information. Numerous examples of records are contained in the Records Retention Schedule. Records do not include unannotated duplicates or convenience copies, non-record drafts, publicly available literature, catalogues and trade journals not published by the Company, informal correspondence, including internal communications or documents created to facilitate meetings or reference materials with no ongoing business or legal value. Note that most email messages and attachments do not become, let alone remain, Records.
Request	Means a request made by a Data Subject to exercise their individual rights under the Data Protection Laws.
Service Provider	Any third-party supplier or vendor that NortonLifeLock contracts with to procure supplies and services.
Special Categories of Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data processed for the purpose of uniquely identifying a natural person, health data and data related to a person's sex life or sexual orientation.
NortonLifeLock	NortonLifeLock, Inc., NortonLifeLock Limited and their subsidiary companies.
NortonLifeLock Data Protection Principles	The privacy principles enumerated on page 1 of the Global Privacy Policy.
Third-Party Distribution and Resale Partners	Third-party partner companies engaged by NortonLifeLock to distribute and resell NortonLifeLock's products and services.
Transfer of data	Means transmission of Personal Data from one country to another either by physical transfer or via remote access across borders, for instance between a European country and a non-European country.

Purpose and scope

The protection of Personal Data, as well as compliance with privacy and data protection laws and regulations, is a constant commitment for NortonLifeLock Ireland Limited and NortonLifeLock, Inc., including its subsidiaries, ("NortonLifeLock", "we", "us"). Capitalised terms used herein and not otherwise defined shall have the meanings assigned to them in the Glossary attached hereto.

NortonLifeLock is a global business and as such we transfer information internationally. We are fully committed to ensuring that there are adequate safeguards in place, as required by the Data Protection Laws, to protect the Personal Data we transfer internationally. As part of this commitment, we have adopted these Binding Corporate Rules, which apply to any intra-group transfer of Personal Data across the world where NortonLifeLock acts as a Data Controller.

These BCR-Cs will apply to the Personal Data NortonLifeLock processes as a Data Controller. NortonLifeLock as a Data Controller will in particular process the Personal Data of its: Employees for employment related purposes; customers; Channel Partners, Distributors, Resellers and other third-parties for NortonLifeLock business related activities; Service Providers for administering and managing relationships; and Consumers.

NortonLifeLock is a truly global organisation, so any Personal Data that are processed in the first place in the EEA are likely to be accessible in the US and, dependent on the purpose of the processing, around the globe.

These BCR-Cs will apply to (i) all NortonLifeLock entities that are party to our intra-group agreement. This agreement ensures that the obligations and safeguards set out in our BCR-Cs and other NortonLifeLock policies are binding on all NortonLifeLock entities and Employees who may process Personal Data (a list of these NortonLifeLock entities is available on our nSight privacy page (ii) all processing of Personal Data by NortonLifeLock throughout the world, regardless of whether it is subject to Data Protection Laws. The third-party beneficiary rights granted by these BCR-Cs are granted to, and enforceable by, Data Subjects.

All Employees and applicable NortonLifeLock entities must ensure they understand and abide by these BCR-Cs when processing Personal Data. These BCR-Cs will be published on NortonLifeLock's website and on the intranet (nSight) for Employees. These BCRs are binding on everyone at NortonLifeLock. In order to ensure our employees, abide by the BCR-Cs and NortonLifeLock's Global Privacy Policy, we inform Employees of their responsibilities and obligations to respect all Personal Data via their employment contract and via regular privacy and security related communications and initiatives, including mandatory annual privacy training.

The table below sets out the nature and purpose of the Personal Data that we process as Data Controller. The information below is to be read, and applies in conjunction with, the NortonLifeLock Global Privacy Statement and NortonLifeLock Product and Service Privacy Notices published at https://www.nortonlifelock.com/privacy/.

Data Subjects	**What Personal Data do we process?**	**Why do we process it?**	**NortonLifeLock's Role**
Consumers	NortonLifeLock may either collect or ask consumers to provide Personal Data such as contact details, including name, mailing address, email address, phone number, shipping and billing information (including credit card and payment information), transaction	NortonLifeLock uses this Personal Data for the purposes below, as well as for related or similar and compatible purposes: to create and manage accounts (e.g. a consumer's Norton Account),	NortonLifeLock Limited acts as a Data Controller for most products and services that it offers to its consumers, within the European Economic Area ("**EEA**").

Data Subjects	What Personal Data do we process?	Why do we process it?	NortonLifeLock's Role
	History, information provided for technical assistance or during customer service interactions, electronic information about computers or devices (including browser type and settings, IP address and traffic data relating to users' internet connection and use of our products). Dependent on the products a consumer purchases, we may also require a consumer to provide additional Personal Data such as bank account details, passwords or usernames and product performance data. Please refer to the Norton Product and Service Notice for further information: https://www.nortonlifelock.com/privacy/	to provision services, to respond to enquiries, to deliver product updates, to convey commercial offerings, to process transactions, to prevent and managed the risk of fraud or other security and safety threats, as well as to conduct research in order to implement product improvements and product updates. Please refer to the Norton Product and Service Notices for further information: https://www.nortonlifelock.com/privacy/	Online purchases on each local country Norton e-store are conducted under the terms of the Global Privacy Policy, under which NortonLifeLock Limited is the Data Controller in respect of Personal Data of EEA Data Subjects.
Customers (including current and prospective customers)	NortonLifeLock may collect or ask customers, to provide Personal Data, such as: • online usage data collected for marketing activities (e.g., geolocation data, cookies data, statistics regarding website usage and browsing preferences, such as language and geographical region); • log data from the products and services used by customers, which may include certain source and destination IP addresses, host name, username, email addresses, URLs, date and time stamps, data volumes, emails and email contents and policy names.	NortonLifeLock processes the Personal Data collected from customers for the following purposes: (a) Management of customer relationship; (b) Marketing of products and services; (c) Development and enhancement of products and services; (d) Compliance with applicable laws, regulations and lawfully issued binding orders and injunctions.	The contracting NortonLifeLock entity acts as a Data Controller for purposes (a) and (e) as detailed in the previous column. For Data Subjects based in the EEA, NortonLifeLock Limited is a Data Controller for purposes (b) to (d) as detailed in the previous column.

Data Subjects	What Personal Data do we process?	Why do we process it?	NortonLifeLock's Role
Employees (both current and prospective and contingent workers)	NortonLifeLock will process Personal Data of our Employees that we may collect during the job interview process, at the start of employment and in the course of employment and such data may include: • name, gender, personal address, phone number and email, emergency contact information, marital / civil partnership status, spouse / domestic partner / dependents details, date of birth, place (country) of birth, nationality, citizenship status and right to work details (including passport details); details of current employment, employment and education history (including, where necessary, details of any background checks), bank account details, driver's license details and photographs; • compensation details, holidays and other leave information (including maternity and sick leave); • any other Personal Data as specified in the applicable Employee Privacy Notice;	NortonLifeLock processes the Personal Data collected from our Employees for recruitment and screening, administration of their employment, administration of compensation and benefits including payroll, provision of HR services, facilitation of global cooperation including communication and provision of a global directory, and as may be required for employment law purposes. NortonLifeLock processes IT Data from Employees for, notably, providing to them IT resources and support, and monitoring the correct functioning and ensuring the security of NortonLifeLock Computer Systems and preventing misuse and outside attacks or threats. Employees should review their applicable Employee Privacy Notice for further details on the types of data we process and why.	Each respective NortonLifeLock employing entity will be the Data Controller for its applicable Employees' Personal Data. Where a NortonLifeLock employing entity shares its Employee Personal Data with another NortonLifeLock entity, the receiving NortonLifeLock entity will in some cases be a Data Controller. For prospective employees, for the purposes of their application the Data Controller will be NortonLifeLock Corporation. Each respective local NortonLifeLock hiring entity will be the Data Controller for local recruitment, onboarding, and any subsequent employment-related processing. Employees can consult their applicable privacy Employee Privacy Notice for details of their Data Controller.

Data Subjects	What Personal Data do we process?	Why do we process it?	NortonLifeLock's Role
	• Personal Data relating to the use by the Employee of the NortonLifeLock Computer Systems, such as username, IP address, emails and other electronic communications, documents, files, websites accessed, and log files of NortonLifeLock Computer Systems usage (IT Data).		
Service Providers (and their Data Subjects)	NortonLifeLock may collect or ask Service Providers to provide Personal Data, such as: • Contact information of persons at suppliers and vendors (e.g., business email address, business postal address, business telephone number and job title).	NortonLifeLock processes the Personal Data collected from vendors and suppliers for administrating and managing the relationship, for provision of the services, billing and account administration, fraud and risk management and as may be required by law.	The NortonLifeLock purchasing entity acts as the Data Controller for the Personal Data it processes for its Service Providers.
Cybercriminals, other Perpetrators of Cyber-Attacks, other Originators of Cyber-Threats, as well as their Targets and/or Victims	NortonLifeLock may process the Personal Data listed below for the purposes of, and to the extent necessary for, ensuring network and information security, including in particular network traffic data related to cyber-threats such as: • sender email addresses (e.g. of sources of SPAM); • recipient email addresses (e.g. of victims of targeted email cyberattacks); • reply-to email addresses (e.g. as configured by cybercriminals sending malicious email);	NortonLifeLock processes this Personal Data for the purposes of, and to the extent necessary for, ensuring network and information security. Both as an organisation in our own right, and as a provider of cybersecurity technologies and services which may include hosted and managed computer emergency and security incident response services, it is in our legitimate interests as well as in our customers', as laid down in Article 6(1)(f) of the General Data Protection Regulation, to collect and process Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring the security of our own, and of our customers' networks and information systems.	For Data Subjects based in the EEA, NortonLifeLock Limited acts as the Data Controller.

Data Subjects	What Personal Data do we process?	Why do we process it?	NortonLifeLock's Role
	• email aliases associated with any of the above; • filenames and execution paths (e.g. of malicious or otherwise harmful executable files attached to emails); • URLs and associated page titles (e.g. of web pages broadcasting or hosting malicious or otherwise harmful contents); and/or • IP addresses (e.g. of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching or other storage of cyber-threats such as malicious or otherwise harmful contents).		
Channel Partners **(e.g. distributors, resellers and other business partners) (and their Data Subjects)**	NortonLifeLock may collect or ask Channel Partners (including their employees, agents and other representatives), to provide Personal Data, such as: • name, job title and level, business email address and other contact details such as, phone number, office address; • login credentials, usernames and other information shared for online usage data (e.g. geo-location data, cookies data, statistics regarding website usage and browsing preferences, such as language and geographical region).	NortonLifeLock processes this Personal Data for the purposes of setting up, administering and managing the relationship with the Channel Partners, including providing Channel Partner membership benefits, contract administration, usage of partner console or web portals, and the sharing of End User Data for sales conversion, lead generation and/or for the sending of marketing communications, regarding NortonLifeLock products, services and events.	The contracting NortonLifeLock entity (or entities as the case may be) will be the Data Controller(s).

Other Data Subjects who access our websites, portals and any other publicly available sources, or otherwise interact with NortonLifeLock	Please refer to the NortonLifeLock Global Privacy Statement for more details

Data Protection Principles

Data protection is very important to NortonLifeLock and we are committed to providing adequate safeguards for the protection of the data protection principles and the fundamental rights and freedoms of individuals within the meaning of applicable data protection law, especially the Data Protection Laws. The privacy principles and commitments set out below embody our approach to data protection and serve as guiding values and steadfast commitments which we are proudly dedicated to.

Lawfulness, Fairness, & Transparency	NortonLifeLock only processes Personal Data in a way that is lawful, fair and transparent. We comply with applicable data protection laws within each of the jurisdictions in which we operate. We are also committed to being transparent about what Personal Data we collect, how we use the Personal Data, with whom we share the Personal Data, what legal basis we are relying upon to process Personal Data, what rights Data Subjects have in respect to their Personal Data and how they can enforce them, and any other information we are required to provide to Data Subjects under Data Protection Laws so that they have a clear understanding of how their Personal Data is handled and protected. We explain all of this information to Data Subjects in a straightforward and clear way in our privacy statement, notices and terms. In the case of Channel Partners and Service Providers, we refer them expressly to our NortonLifeLock & Norton Global Privacy Statement so as to enable them to inform their relevant employees, agents, representatives and other Data Subjects whose Personal Data is collected and processed by us. We review our privacy statement, notices and terms regularly to keep them up to date and to ensure they match our internal practices. **Channel Partners:** Please refer to our NortonLifeLock Global Privacy Statement for further details. **Consumers**: Please refer to our Product Privacy Notices which are to be read and apply in conjunction with, and in addition to the NortonLifeLock Global Privacy Statement. **Current and Prospective Employees:** Should refer to the Applicant Privacy Notice or their respective Employee Privacy Notices for further details. **Service Providers, Cyber Criminals/Victims and other Data Subjects**: Should refer to our NortonLifeLock Global Privacy Statement for further details. We only process European Personal Data where we have a lawful basis for such processing under Data Protection Laws. The lawful basis relied upon for processing the Personal Data of each category of Data Subject in each use case is contained in our privacy statement, notices and/or terms. **Processing of Special Categories of Personal Data** We only process Special Categories of Personal Data where we can rely on an appropriate legal basis for such processing as provided for under Data Protection Laws. The legal basis we rely upon for processing Special Categories of Personal Data will be notified to Data Subjects in our privacy notices. Special Categories of Personal Data are subject to heightened information security standards, and correspondingly increased technical and organisational measures.

Purpose limitation	We only collect Personal Data for specified, clear and legitimate purposes and do not process it in a manner incompatible with or disproportionate to those purposes. We ensure privacy is embedded and considered in all our business decisions and we regularly assess whether Personal Data we collect is necessary for our identified, specific purposes. One of the ways in which we achieve this is by appointing Privacy Business Leads for each NortonLifeLock product, service, and corporate function. Privacy Business Lead's role is to act as a liaison between Privacy Legal and the business functions. The Product organization or other responsible team is also responsible for completing a preliminary Data Protection Impact Assessment (Pre-DPIA) questionnaire for every new or changing processing activity, and where necessary completing a full Data Protection Impact Assessment (**DPIA**). NortonLifeLock shall escalate concerns to Privacy Legal, applicable Committees and DPO where appropriate, to ensure that processing activities are always specific, limited and proportionate to what is necessary, and pursued for legitimate purposes only.

Data Minimization and Accuracy	We only collect as much Personal Data as is adequate, relevant, and necessary to achieve the purposes for which it is collected. We take steps to ensure that, as and where relevant, the Personal Data we hold is accurate, up-to-date, and complete as well as ensuring Personal Data that is inaccurate is duly rectified or erased. In some instances, Consumers have access to and control of what Personal Data is processed so they can review, amend, or remove their Personal Data as they wish. Consumers can also contact Norton Support respectively to amend, rectify or remove any personal details that may not, or no longer be accurate, relevant or necessary.

Retention	We do not retain Personal Data in an identifiable form for longer than is necessary for the purpose(s) for which we originally collected them, unless Data Protection Laws requires us to maintain it. We have implemented data retention policies which set out the appropriate time periods for which we retain Personal Data. We will hold Personal Data on our systems for the longest of the following periods: 1. As long as necessary to maintain our ongoing business relationship, or as needed to provide Data Subjects with the products, services or information which they are entitled to or can otherwise reasonably expect to receive from us; 2. For as long as necessary for the purpose for which we collected it or for which the Data Subject supplied it to us in accordance with any product or service relevant activity or process; 3. Any retention period that is necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements; 4. The end of the period in which litigation or investigations might arise in respect of our business relations or other interactions with Data Subjects.

Security (Integrity and confidentiality)	Security of Personal Data is crucial to NortonLifeLock's business. NortonLifeLock ensures that Personal Data is protected and processed carefully and securely. We use appropriate technical and organisational measures to keep Personal Data secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage and to ensure its integrity, confidentiality and availability across all systems at all times, in consideration of the evolving risk facing them. We have implemented appropriate security measures and company policies, which are regularly reviewed for accuracy and compliance with industry standards. Examples of some of the security measures we take include the following: **Physical Safeguards** We lock doors and file cabinets, control access to our facilities, implement a clean desk policy, and apply secure destruction to media containing Personal Data. **Technology Safeguards** We use network and information security technologies such as NortonLifeLock anti-virus and endpoint protection software, encryption, intrusion detection and data loss prevention, and we monitor our systems and data centres to ensure that they comply with our security policies. For example, confidential information such as credit card data is transmitted using Transport Layer Security ("TLS") encryption. **Organisational Safeguards** We conduct regular company-wide, as well as role-specific and targeted training, awareness programs and exercises on security and privacy, to make sure that our employees and contractors understand the importance of protecting Personal Data, and that they learn and maintain the necessary knowledge and skills effectively to protect it in practice. Our organisational privacy policy and standards also guide our handling of Personal Data. NortonLifeLock ensures the same high levels of security and protection are afforded to the Personal Data of our customers, our Consumers, our Employees, our Service Providers, our Channel Partners, as well as of Cyber Criminals/Victims and other Data Subjects when we use third-parties or subcontractors. Any sharing of Personal Data with such third-parties shall be subject to a contract which contains the contractual clauses mandated by General Data Protection Regulation's Article 28, including an obligation to notify us of Personal Data Breaches. We will, within 72 hours and/or within applicable regulatory deadlines and conditions, notify relevant Data Protection Authorities, and if appropriate inform Data Subjects, including Consumers, Employees, Service Providers, Channel Partners, and, as relevant, other Data Subjects, of Personal Data Breaches significantly affecting them. We also keep a detailed record of all data security incidents which involve Personal Data and shall make that record available to Data Protection Authorities, where required to do so.

Accountability	Each NortonLifeLock entity is responsible and accountable for upholding these NortonLifeLock Data Protection Principles and for respecting individuals' privacy rights in line with our corporate governance structure. In order to create an environment of trust and to comply with Data Protection Laws, all individuals operating within or on behalf of NortonLifeLock must comply with these BCR-Cs and help NortonLifeLock to uphold its commitments to the protection of Personal Data. This commitment is further highlighted in "**How NortonLifeLock Ensures Privacy Compliance"**. NortonLifeLock maintains a record of processing activities carried out on Personal Data which may be made available to Data Protection Authorities as required. We also carry out Data Protection Impact Assessments where we propose engaging in processing activities that could result in high risks to the rights and freedoms of Data Subjects and shall consult relevant Data Protection Authorities in relation to such proposed processing activities when required to do so by Data Protection Laws. To the extent required by Data Protection Laws, each NortonLifeLock entity implements appropriate technical and organisational measures designed to ensure compliance with NortonLifeLock Data Protection Principles and these BCR-Cs. We ensure that any complaints made by Data Subjects are promptly handled as per our complaint process detailed below at 'Questions, Complaints or Concerns'.

Additional Commitments

Data Subject Rights

We are committed to addressing the rights of individuals with respect to our processing of their Personal Data in accordance with Data Protection Laws. Under Data Protection Laws, Data Subjects have the following rights:

1. the right to access and obtain a copy of Personal Data relating to them;
2. the right to rectify, erase or restrict the processing of Personal Data if it is incomplete or inaccurate, or no longer necessary for the purpose for which it was collected or retained;
3. the right to object to the processing of their Personal Data in certain circumstances;
4. the right to move, copy or transfer Personal Data in certain circumstances;
5. where their consent has been obtained for processing Personal Data, the right to withdraw such consent;
6. the right to be informed;
7. the right to data portability; and
8. rights in relation to automated decision making and profiling.

All requests to exercise these rights should follow the processes described in the section below on 'Questions, Complaints or Concerns'.

Transfers to Third-Parties

Where we transfer Personal Data to third-parties outside the NortonLifeLock group, we ensure that the required contractual obligations and the NortonLifeLock Data Protection Principles are stipulated to and abided by such third-parties.

Where we transfer Personal Data to third-parties located in countries outside of the EEA that do not offer an adequate level of Personal Data protection, we ensure that appropriate safeguards are put in place to protect the Personal Data, as required by Data Protection Laws. Please see the 'Third-Party-Processing' section below for further information on such data transfers.

Third-Party-Processing

Prior to permitting any Data Processors or sub-processor to process Personal Data on its behalf, NortonLifeLock carries out an appropriate, comprehensive due diligence process to assess whether such third-parties have appropriate procedures in place to protect the Personal Data in accordance with Data Protection Laws.

NortonLifeLock ensures that any external Data Processors, or sub-processors as may be applicable, only process Personal Data if they have entered into appropriate contractual terms with NortonLifeLock that require:

1. Personal Data to be processed in accordance with applicable data protection laws (in particular the mandatory contractual requirements contained in Article 28 of the GDPR) and our BCR-Cs;
2. Personal Data to only be processed on the instructions of NortonLifeLock;
3. the Data Processor to implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised access, loss or disclosure;
4. NortonLifeLock to be informed (a) if there is a Personal Data Breach which impacts NortonLifeLock Personal Data, (b) if the Data Processor cannot comply with its data protection obligations and (c) if it receives a request or complaint from a Data Subject; and
5. any sub-processing to be subject to NortonLifeLock's consent and subject to an agreement in place with the sub-processor containing terms which ensure the same level of protection for the Personal Data as those terms in the agreement NortonLifeLock has in place with the Data Processor.

Any external Data Processor or sub-processor located outside of the EEA (or that may process Personal Data outside the EEA) in countries that are not recognised by the European Commission as offering an adequate level of Personal Data protection, and which is acting on behalf of NortonLifeLock , will be required to ensure that such transfers are covered by alternate appropriate safeguards, specifically standard data protection clauses adopted by the European Commission. If applicable, Data Subjects may obtain copies of such safeguards by contacting NLL_privacy@nortonlifelock.com.

Where a NortonLifeLock entity uses an internal Data Processor (i.e. another NortonLifeLock entity) to process

Personal Data on its behalf and under its instructions, the processing shall be in accordance with these BCR-Cs.

Training

These BCR-Cs are binding on everyone at NortonLifeLock. In order to ensure our Employees abide by these BCR-Cs and NortonLifeLock's Global Privacy Policy, we inform Employees of their responsibilities and obligations to respect all Personal Data via their employment contract and via annual regular privacy and security related communications. NortonLifeLock ensure that all employees participate in annual privacy and security training and there is a system lockout consequence for employees who do not complete training within the specified timeframe. We also provide specific training to Employees whose role may require more tailored training.

The Privacy Legal team and related departments are responsible for ensuring that all employees undertake the mandatory training. Employees are also required to abide by NortonLifeLock's Data Protection Principles, which are integrated into NortonLifeLock's Code of Conduct, and employees are required to undertake mandatory annual training for NortonLifeLock's Code of Conduct.

The protection of Personal Data of Data Subjects is fundamental to preserving trust. To ensure Employee compliance with the NortonLifeLock Data Protection Principles and these BCR-Cs, NortonLifeLock has a Code of Conduct and Global Privacy Policy, through which Employees are informed that any violation will result in disciplinary action, subject to applicable local laws.

Employee accountability is a key element of NortonLifeLock's Global Privacy Policy, which requires Employees to ensure that they:

- are able to identify Personal Data, which is clearly defined;
- abide by the principles and requirements of the General Data Protection Regulation, including minimal collection and use;
- actively participate in managing data appropriately after processing (in particular, that they keep it up-to date, accurate and secure);
- learn to properly handle, access, and dispose of data as appropriate and abide by NortonLifeLock data handling and security polices;
- adopt and follow Privacy by Design practices and controls;
- use data for legitimate business purposes only;
- manage applications and technology appropriately;
- ensure Data Processors and sub-processors abide with our security and privacy requirements; • report data security incidents to relevant stakeholders; and
- complete required training.

Audit

NortonLifeLock regularly assesses and audits compliance with these BCR-Cs, both via internal and external audits by our Data Protection Officer (DPO) and competent Data Protection Authorities. We also achieve certifications such as the ISO from accredited third-party organisations.

NortonLifeLock conducts data protection audits on a regular basis or upon the request of the DPO, EEA Data Protection Oversight Committee. and the Audit Committee of the Board of Directors. The audit programme is comprehensive and covers all aspects of these BCR-Cs, including methods of ensuring that corrective actions will take place. The results of audits are communicated to the Global Head of Ethics and Compliance, the Privacy Legal team, the Internal Audit team, the Ethics and Compliance Steering Committee, the EEA Data Protection Oversight Committee and to the board of NortonLifeLock, Inc.

Third-Party Audits and Certifications

As a general point of reference, NortonLifeLock contracts with independent organisations and achieves certifications for the portions of our business that warrant such evaluation. NortonLifeLock has selected as its information security model the best practice control framework defined in the international Standard ISO 27001Information Security Management System (ISMS) Requirements. In order to meet the needs of our customer base and maintain a high level of service and security, NortonLifeLock typically provides our ISO 27001 certificate as well as the results of the annual SOC Type II attestation conducted by our external auditors (under non-disclosure agreements) in lieu of having multiple third-party assessments performed throughout the year. NortonLifeLock has determined that this approach provides significant value to a variety of customers and prospects, particularly those in the financial services and other heavily-regulated industries, while preserving the confidentiality of each Data Controller’s Personal Data in NortonLifeLock’s multitenant environments and preventing disproportionate constraints on NortonLifeLock’s resources.

Internal Audits

NortonLifeLock's current data privacy compliance function falls within the scope of our dedicated EEA Data Protection Oversight Committee our DPO and the Privacy Legal Team, which all provide ongoing advice and support to ensure compliance with data privacy regulations and frameworks. NortonLifeLock's ongoing compliance with these BCR-Cs and our data privacy program are centralised under our Internal Audit Office. The Internal Audit Office is responsible for ensuring that our committed standards, including BCR-Cs, are upheld, and applied consistently across NortonLifeLock.

Internal audits are carried out annually, and are determined by the Privacy Legal team, in connection with the

Internal Audit Office and the Global Cyber Security team, and where required or relevant, the DPO. The Internal Audit Office leads and directs any relevant internal audits.

NortonLifeLock's internal audits cover NortonLifeLock's key systems, products and applications that process

Personal Data, onward transfers, decisions taken as regards mandatory legal requirements that conflict with these BCR-Cs, review of the contractual terms used for transfers out of the group, BCR-C terms and documentation, incident response planning and supplier security and data privacy rigour. The internal audit process is clearly set out in internal procedure documents.

Cooperation

Where required, NortonLifeLock will co-operate with, accept to be audited by, and agree to respond and comply with the advice of Data Protection Authorities on any issue related to these BCR-Cs.

Questions, Complaints or Concerns

Where we receive a Data Subject complaint, question or concern relating to our responsibilities as Data Controller, we will handle such request in accordance with our usual procedures for complying with Data Subject requests outlined below which are included in our *Privacy Request and Complaint Handling Standard*.

NortonLifeLock Complaint Procedure

1. Where Data Subjects wish to make a complaint, in the first instance, they should make a complaint to the relevant teams in NortonLifeLock. We can be reached at the following contact details:
    - NortonLifeLock customers: https://support.norton.com/sp/en/uk/home/current/contact?src=support&type=support
    - Employees: should contact their People Manager
    - Any other complaints: nll_privacy@nortonlifelock.com
2. NortonLifeLock will use reasonable endeavours to acknowledge receipt of a complaint within 5 working days and will deal with a complaint without undue delay and in any event within one (1) month of receipt of the complaint. NortonLifeLock may request an extension of two (2) months to respond to a query if the circumstances are complex in nature but this does not preclude the right of the Data Subject to contact his/her Data Protection Authority if he/she thinks his/her rights have been violated.
3. If NortonLifeLock concludes a complaint is justified then the Privacy Legal Team will work with the Data Subject to resolve the matter and where applicable (and if needed in consultation with the DPO) ensure that any relevant processes, policies or procedures that resulted in any non-compliance with these BCR-Cs are amended in timely manner to restore and ensure ongoing compliance.

4. Data Subjects can also lodge any complaints they have with our DPO using the following contact details: dpo@nortonlifelock.com.

Remedies

If NortonLifeLock rejects or is unable to resolve a complaint from an individual residing in the EEA or otherwise protected by Data Protection Laws, the individual has the right to lodge the complaint before the Data Protection Authority competent for the relevant NortonLifeLock entity or if that is not possible, the complaint can be lodged to the Data Protection Authority in the individual's country of habitual residence, place of work or the place of the alleged infringement.

In addition to the right to make a complaint as described above, Data Subjects can also seek redress by:

(1) seeking a judicial remedy or claim for compensation in the courts of competent jurisdiction of the relevant NortonLifeLock entity (for non-EEA NortonLifeLock entities, NortonLifeLock Limited is the relevant NortonLifeLock entity) or the courts in the Data Subject's own jurisdiction,

(2) lodging a complaint directly with a competent Data Protection Authority.

Individuals may claim more favourable remedies if these exist under local law.

NortonLifeLock Ireland Limited accepts all responsibility for and agrees to take necessary action to remedy the acts of non-EEA NortonLifeLock entities, including providing compensation for material or non-material damages caused by a violation of the BCR-Cs by such non-EEA entities in circumstances where a Data Subject is entitled to be compensated.

The burden of proof is on NortonLifeLock Ireland Limited to prove otherwise, i.e. demonstrate that NortonLifeLock Ireland Limited is not liable for any alleged violations of these BCR-Cs. In order to do this, NortonLifeLock Ireland Limited must demonstrate that either the violation did not occur, or that NortonLifeLock was not responsible for the alleged violation.

How NortonLifeLock Ensures Privacy Compliance

NortonLifeLock has a Global Ethics & Compliance Steering Committee, an EEA Data Protection Oversight Committee, and a corporate-wide privacy operating model in place that are responsible for overseeing and ensuring compliance with these BCR-Cs. Different stakeholders at all levels of the organisation play a role in ensuring overall privacy risk management and data protection compliance.

The NortonLifeLock Privacy Operating Model is led by the Head of Compliance of the organisation, who reports directly to the Board of Directors and reports regularly to the Ethics and Compliance Steering Committee.

The EEA Data Protection Oversight Committee (**EEA DPOC**) has a mandate to cascade privacy through the Group with support from Privacy Legal, advise respective business areas on how to implement privacy by design to mitigate privacy risks, including ensuring that the data protection impact assessment process and recommendations of the privacy team are followed and implemented.

The Global Ethics & Compliance Steering Committee's privacy mandate includes; to manage and resolve issues escalated by the EEA DPOC, to elevate the ownership privacy governance to the executive level and align privacy to business needs and priorities and follow privacy developments impacting the business.

NortonLifeLock has engaged an independent external DPO to support the privacy management program. The DPO reports into NortonLifeLock's Ethics and Steering Committee, which includes the Head of Legal as well as senior management from audit and risk. The DPO's role includes; cooperating with supervisory authorities and

acting as the principal contact point, informing and advising the organisation regarding data protection compliance, monitoring compliance with the GDPR and national data protection laws as well as with the policies of the organization in relation to the protection of personal data.

The Privacy Legal team advises the business on data protection law compliance and supports the business' implementation of privacy by design by reviewing and approving pre-DPIAs in respect of NortonLifeLock products and vendor relationships. The Privacy Legal team update and review privacy policies, procedures and standards and support the wider legal team in negotiating data protection contract terms.

Privacy Business Leads have been appointed across business functions to; embed privacy compliance within the business, act as the extended voice of the privacy team, provide privacy related guidance to respective departments, act as a point of escalation for matters that require Steering Committee approval, carry out and review data protection impact assessments at first instance.

The Privacy Operation Compliance Function is tasked with operationalizing global privacy function.

The Global Cyber Security team is responsible for ensuring that NortonLifeLock's security standards are incorporated into products and services, and that adequate protections are in place for personal data that is processed by NortonLifeLock and by NortonLifeLock's subcontractors.

Enforcement and Liability

Liability

Each NortonLifeLock entity is responsible for complying with these BCR-Cs.

In addition, NortonLifeLock Ireland Limited accepts all responsibility for and agrees to take necessary action to remedy the acts of non-EEA NortonLifeLock entities, including providing compensation for material or non-material damages caused by a violation of these BCR-Cs by such non-EEA NortonLifeLock entities in circumstances where a Data Subject is entitled to be compensated. If a non-EEA NortonLifeLock entity violates the terms of these BCR-Cs, Data Subjects will be able to seek to enforce their right and remedies against NortonLifeLock Ireland Limited before the courts in Ireland or the courts in the jurisdiction where the Data Subject has his or her habitual residence and/or can raise the issue with the competent Data Protection Authority of the Data Subject's habitual residence, place of work or place of the alleged infringement.

Enforcement

These BCR-Cs apply to all processing of Personal Data within NortonLifeLock throughout the world. The third-party beneficiary rights granted by these BCR-Cs are granted to, and enforceable by, Data Subjects.

1. Individuals' Third-Party Beneficiary Rights

Data Subjects have third-party beneficiary rights and can seek certain judicial remedies and receive compensation for damages directly against any EEA NortonLifeLock entity and against NortonLifeLock Ireland Limited for any non-EEA entity should it fail to meet its following obligations:

- comply with the NortonLifeLock Data Protection Principles outlined above including with regard to transfers of Personal Data outside of the EEA;
- ensure Data Subjects are appropriately and clearly informed about the processing of their Personal Data by NortonLifeLock, including having easy access to a copy of these BCR-Cs;

- comply with the various rights of Data Subjects in accordance with Data Protection Laws including the right of access to their Personal Data, the rights to rectify, erase, restrict or object to the processing of Personal Data and the right not to be subject to decisions based solely on automated processing, including profiling;
- be transparent and notify relevant Data Protection Authorities where a national legal requirement prevents a NortonLifeLock entity from complying with these BCR-Cs;
- inform Data Subjects of the right to complain through NortonLifeLock's internal complaint procedures;
- cooperate with relevant Data Protection Authorities to ensure compliance with these BCR-Cs;
- notify Data Subjects of their right to lodge a complaint about NortonLifeLock's processing of Personal Data with NortonLifeLock Ireland Limited and/or the relevant Data Protection Authority or before the courts of competent jurisdiction of the relevant NortonLifeLock entity or the courts in the jurisdiction where the Data Subject has his or her habitual residence;
- notify Data Subjects of their right to obtain redress, and where appropriate, compensation for a violation of these BCR-Cs;
- notify Data Subjects of the procedures to be followed if they are reporting to a Data Protection Authority about legal requirements which a NortonLifeLock entity is subject to and which are likely to have a substantial adverse effect on guarantees provided in these BCR-Cs.

Proving Liability

Where a Data Subject can demonstrate that he/she has suffered damage and he/she can demonstrate that it is likely that the damage has occurred because of a violation by NortonLifeLock of these BCR-Cs, the burden of proof is on NortonLifeLock Ireland Limited to prove otherwise, i.e. demonstrate that NortonLifeLock Ireland Limited is not liable for any alleged violations of these BCR-Cs. In order to do this, NortonLifeLock Ireland Limited must demonstrate that either the violation did not occur, or that NortonLifeLock was not responsible for the alleged violation.

Changes to these BCR-Cs

NortonLifeLock may modify these BCR-Cs or the list of NortonLifeLock entities that are party to our intra-group agreement if, for instance, the regulatory environment or the company structure changes. Such modifications will be brought to the attention of the NortonLifeLock group and the Data Protection Authorities as soon as possible following the amendment together with a brief explanation of the reasons justifying the modifications. No transfer will be made to a new NortonLifeLock entity until the new entity is effectively bound by and can comply with these BCRs.

Conflict of Laws

If a NortonLifeLock company becomes aware of existing or future legislation applicable to it that prevents or will prevent it from fulfilling its obligations under these BCR-Cs, it will promptly inform NortonLifeLock Ireland Limited and the Data Protection Authority competent for the relevant NortonLifeLock company unless prohibited by Data Protection Laws or by a lawfully issued compelling order.

If a NortonLifeLock company is subject to a legal requirement (including a request from a law enforcement authority or State security authority compelling disclosure of Personal Data) it will promptly notify NortonLifeLock Ireland Limited. Where the legal requirement is likely to have a substantial adverse effect on the

guarantees contained in these BCR-Cs, unless prohibited by Data Protection Laws or by a lawfully issued compelling order, the NortonLifeLock company will promptly notify NortonLifeLock Ireland Limited and the competent Data Protection Authority of the nature of the requirement, its origin and the legal basis for disclosure. Compliance with the legal requirement shall be suspended during this period. If this notification and/or suspension is prohibited by Data Protection Laws or a lawfully issued compelling order, the relevant NortonLifeLock company will use reasonably efforts to procure a waiver of this prohibition in order to facilitate the sharing of information in relation to the requirement.

To the extent NortonLifeLock is unable notify the competent Data Protection Authority about such requirements, NortonLifeLock shall on request and on an annual basis, provide competent Data Protection Authorities with general information on the receipt of such legal requirements for disclosure of Personal Data.

We will comply with Data Protection Laws when processing Personal Data. Where Data Protection Laws require a higher level of protection for Personal Data than is provided for in these BCR-Cs, such Data Protection Laws will take precedence.

We will ensure that any transfers of Personal Data to any public authority will not be disproportionate or indiscriminate in a manner which would go beyond what is necessary in a democratic society.