GEN DIGITAL GLOBAL PRIVACY STATEMENT

1. Introduction

When it comes to your personal data, Gen Digital Inc. and its subsidiaries (collectively referred to as "Gen Digital", "Norton", "LifeLock", "we", or "us"), as well as our employees, contractors, and service providers, are committed to providing you with transparency. We process personal data in accordance with applicable legislation.

This Privacy Statement ("Statement") applies to the Gen Digital websites, services, and products (our "Services") that link to or reference this Statement. In this Statement, we describe how we collect, process, use and disclose personal data, and your rights and choices regarding our processing of your personal data.

Additional information on our personal data practices may be provided in product descriptions, contractual terms, supplemental privacy statements, or notices provided prior to or at the time we collect your personal data. Please see https://www.nortonlifelock.com for more details.

If you are in the European Economic Area, and unless stipulated otherwise contractually, the Controller of your personal data is:

NortonLifeLock Ireland Limited
Ballycoolin Business Park
Blanchardstown
Dublin 15
Ireland D15E867

2. Categories of Personal Data We Collect:

We collect personal data about you from different sources as listed below. In this Statement, "personal data" means any information relating to an identified or identifiable individual.

Personal Data You Provide to Us

When you interact directly with us, we may collect personal data that you provide to us, including:

User Data. If you create an account with us, make a purchase, or request information about our product we collect information about you, including:

- **Account Data**. If you create an account with us, we collect identifiers, such as your name, mailing address, email address, phone number, user credentials (login name and password), and depending on the product purchased may also collect child name and age, emergency contact information, and location identifying labels (such as "home" or "school," as defined by parent), driver's license, and date of birth, as well as your audio, electronic, visual, or similar information, such as your picture (or avatar, if chosen).
- **Payment Data**. If you complete a purchase for one of our products and services, we collect your billing address, including credit card, debit card, and or PayPal payment

data, National ID (region specific, if outside the United States), and VAT/Tax ID (regional specific, if outside the United States), as well as commercial information, such as information about the items you have purchased.

- **Identity Data**. We collect your date of birth, age, and gender, as well as identifiers, such as your address, email, bank account information, credit/debit card information, mother's maiden name, insurance information, gamer tag, and other personal details about you, such as your Social Security Number and/or state/government identifier, driver's license number or other national personal identifier to verify your identity and to provide identify theft monitoring and protection services.
- **Communications**. If you contact us directly, we collect personal data about you, including identifiers, such as your name, email address, phone number, the contents of any message or attachments that you may send to us, and any other information you choose to provide. We may retain and review audio, electronic, visual, or similar information, such as audio call and chat recordings and/or the contents of the messages as required/permitted by law and our recording and information management policies. We will also collect identifiers from you, such as your email address and phone number, when you sign up to receive product updates, offers, and other promotional information or messages from us. When we send you emails, we may track whether you open them to learn how to deliver a better customer experience and improve our Services.

User Content. We operate forums, websites, and related information services, to better assist you in using our Services, discussing technical issues, and sharing your experiences. You should be aware that any data you provide in these public forums will be read, collected, and used by others who access them. To request removal of your personal data from any forum, contact us here. In certain circumstances, we may not be able to remove your personal data, in which case we will let you know why. Please note that your use of these community services may be subject to additional terms and conditions.

Careers. If you decide that you wish to apply for a job with us, you may submit your contact information and your resume online. We will collect the Professional or Employment-Related Information you choose to provide on your resume, such as your education and employment experience**.** You can find our Applicant Privacy Statement here.

Personal Data We Collect Automatically

When you visit and use our websites and Services, we may automatically collect data about your interaction with our websites and Services, including:

Product Data. If you install our products, we collect information about you, including:

- **Device Data.** We collect information to facilitate installation and use of our products, including your device and system information such as operating system, device name, browser, network, and applications running on the device. This data can also include internal identifiers such as Wallet ID, Auto bill ID, payment transaction ID, serial numbers, MAC address, Norton Machine ID, account generated unique ID, mobile device IDs (UDID, IMEI, and IDFA), Wi-Fi MAC Address, install identifier, Member ID, and LifeLock ID.

- **Service Data.** This can include product license information, usage data, and/or preference information, browser activity, and URLs accessed, restoration case number

(for filed restoration cases only), complaint case number (for lodged complaint only), parent case numbers (for disputed alerts only). This data may include internet or other electronic network activity information, such as diagnostic data such as crash dumps, system logs, error reports, product and internet usage time, network connection activity, interactions with our websites and extensions, blocked websites, device or phone settings, and reviews from third parties which we collect to, as necessary, to troubleshoot any malfunctioning Services. This data also helps us better understand and better serve your interests, expectations, needs and requirements.

- **Security Data**. This data may include financial transactions, alert data, and data that is collected for cyber threat intelligence, as needed to provide cyber safety and identity threat protection Services. This data can include URLs and websites visited, executable files identified as malware, application names and versions, your interface and screen activity, and search terms. This data can also include device fingerprint ID from third parties to validate and authenticate payment and transaction information related to billing on accounts.
- **Geolocation Data**. When you use our Services, if you consent via the device interface to sharing the precise geolocation data of your device, we will receive your precise location information. We also infer your more general location information (for example, your IP address or time zone may indicate your more general geographic region).
- **Network Traffic Data**. We may process internet or other electronic network activity information, such as network traffic data related to cyber and identity threats for network and information security purposes, including:
    - Sender email addresses (e.g., of sources of SPAM such as phishing scams);
    - Recipient email addresses (e.g., of victims of targeted email attacks);
    - Reply-to email addresses (e.g., as configured by cybercriminals sending malicious email);
    - 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 content);
    - IP addresses (e.g., of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching, or other storage of cyber and identity threats such as malicious or otherwise harmful content); and
    - Browser information (e.g., user agent string and session within cookies).

  Depending on the context in which such data is collected, the data may contain personal data concerning you or third parties. However, in such cases, we will process the data only to the extent strictly necessary and proportionate to the purposes of detecting, blocking, reporting (by removing any personally identifiable elements), and mitigating the cyber or identity threats of concern or those of other users relying on our Services to protect their networks, systems, and identities. When processing personal data in this

context, we will only identify specific data subjects if and to the extent necessary for the remediation of the cyber or identity threats concerned, or as required by law.

Website Data. When you browse our websites and Services, we automatically collect internet or other electronic network activity information, commercial information, and inferences drawn from personal information about the individual web pages or products that you view, the purchases you make, what websites or search terms referred you to our Services, the dates and times of your visits, and other information about how you interact with our Services. When you browse our websites and services, we may collect personal data using cookies and similar technologies (e.g., web beacons). Please see our Cookie Statement for more details.

Personal Data We Collect from Other Sources

- **Referrals**. We may collect personal data from you about other people, such as personal data about friends and family through customer or employee referrals, or data about family members you include on your account.

  When you choose to provide us with personal data about third parties, we will only use this data for the specific stated reason that you provided it. It is your responsibility to abide by applicable privacy and data security laws when you disclose third parties' personal data to us, including informing third parties that you are providing their personal data to us and how it will be transferred, used, or processed, and securing the appropriate legal permissions and safeguards. If you choose to provide us with a third party's personal data, you represent that you have the third party's permission to do so. Examples include forwarding references or sending job referrals. You also acknowledge that when we interact with such third-party individuals whose personal data you share with us, it is our duty to inform them that we obtained their personal data from you. Where applicable, third parties may unsubscribe from any future communication following the link provided in the initial message. If you believe that one of your contacts has provided us with your personal data and you would like to request that it be removed from our database, please contact us.

- **Third-Party Data**. This information includes personal data we may obtain about you from a third party through the use of our Services, including:

  - Credit reporting agencies and financial institutions (used for purposes such as identity theft protection Services);
  - Enrollment information from your employer (when enrolled with our Services as an employee benefit);
  - Marketing and joint-marketing partners (used for purposes such as to offer Services and/or joint Service bundles to prospective members);
  - Public sources such as the dark web to alert you to potential misuse of your personal data; and
  - Private sources for purposes of providing customers with alerts related to financial transactions, property title, social media abuse, and other types of alerts within our products.

Such data includes threat intelligence data used to analyze threats and protect you, us, and our other customers against cyber threats. This data may include the email and IP address of the sender of malware. Third Party data may also include data reflecting your usage of and engagement with our websites and Services collected by us or third-party analytics providers. This data helps improve the functionality and effectiveness of our websites and Services and may help to better tailor our websites and Service to your usage and preferences. You can find more information about sharing of your personal data with third-party partners in the "When and Why We Disclose Your Personal Data" section below.

We may combine personal data from our partners and third parties with personal data we already have about you, to provide you with more relevant communications and to better tailor our offers to you. We make reasonable efforts to verify that the third parties we work with are reputable, and we do not ask them to disclose your personal data if we do not have a lawful purpose and valid legal basis to collect and process that data.

3. How We Use and Process Your Personal Data

We process your personal data:

Where it is necessary to fulfill our contract with you at your request, in order to:

- Create and manage your account;
- Provide you with information and Services that you request;
- Authenticate your identity prior to enrolling in our Services;
- Verify your identity and entitlement to Services, when you contact us or access our Services;
- Process your purchase transactions;
- Update you on the status of your orders;
- Allow you to register the Services you purchase;
- Confirm that you received necessary service and transactional emails;
- Manage your subscriptions; and
- Provide you with technical and customer support.

Where you have provided your consent, in order to:

- Subscribe you to newsletters and send you product updates or technical alerts;
- Send you marketing communications and information on new Services;
- Communicate with you about, and manage, your participation in contests, offers, or promotions;
- Solicit your opinion or feedback and/or provide opportunities for you to test Services;

- Enable you to refer a friend who may be interested in our offerings, as permitted by law;
- As applicable, to enable non-essential cookies or similar technologies; and
- As applicable, to provide you with interest-based ads about Gen Digital on sites other than our own.

For the purpose of fulfilling our legal obligations, we may be obligated to, for instance, keep and process records for tax purposes, accounting, other obligations such as court or other legal orders, and other necessary disclosures.

For the purpose of promoting and operating our business and advancing our or a third party's legitimate interests, such as the effective delivery of our Services, and communications to you as well as to our other customers and partners, in order to:

- Enable participation in interactive features of our Services;
- Notify you about changes to our terms or this Privacy Statement;
- Communicate commercial promotions and provide quotes for our Services;
- Inform you about additional Services that provide solutions to issues detected;
- Promote and administer co-branded offers with trusted partners;
- Confirm sales conversions and conduct lead generation activities;
- Better administer and understand the usability, performance, and effectiveness of our Services websites, and communications to you, including troubleshooting, debugging, reviewing customer service interactions, data analytics, testing, research, and statistical analysis;
- Improve our Services (including developing new Services) and customize and present content in the most relevant and effective manner for you and for your device, including suggestions and recommendations about things that may be of interest to you;
- *Enhance the security of our own networks and information systems;
- *Develop cyber-threat intelligence resources; and
- *Otherwise keep our Services, business, and users safe and secure, and comply with applicable laws and regulations or judicial process or government agencies, and to protect or exercise our legal rights and defend against legal claims.

***For Network and Information Security Purposes and Cyber-Threat Intelligence:**

Our legitimate interests include developing threat intelligence resources aimed at maintaining and improving the ability of our information networks and systems to resist unlawful or malicious actions and other harmful events, such as cybercriminal activities, and attempts at identity theft or fraud ("cyber and identity threats").

We only rely on our or a third party's legitimate interests to process personal data when these interests are not overridden by your rights and interests.

4. When and Why We Disclose Your Personal Data

We are committed to maintaining your trust, and we want you to understand when and why we disclose personal data to third parties. We do not sell your personal data or use or disclose sensitive personal information for purposes other than those set forth in the California Consumer Privacy Act ("CCPA"). Data obtained through short code programs will not be shared with any third-parties for their marketing reasons/purposes. We may disclose the categories of personal described above in "Categories of Personal Data We Collect" to the entities and for the purposes described below.

We may disclose personal data about you with your consent, or:

- **With our Partners**

  We may provide your personal data to our partners for the purpose of allowing them to conduct Gen Digital business. Our partners may use your personal data to communicate with you and others about Gen Digital Services either alone or jointly with partner products and services. We may provide your personal data to partners to confirm your eligibility for joint or co-branded offers or to communicate and administer such offers (e.g., report sales conversions, verify eligibility, assess effectiveness of joint offer, etc.). Our partners are not allowed to use any data including personal data that they receive from us for any purpose except for communicating, evaluating, improving, and administering the offer in question (Gen Digital branded, co-branded, or joint offer). This will not affect the partner's ability to use personal data that it may already have obtained from you or other sources. If you do not wish to receive promotional emails from our partners, you can unsubscribe directly using the unsubscribe link or tool provided in the partner's email or other communication to you.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our partners: User data, Product data, Website data, Third-party data.

- **With our Distributors or Resellers**

  We may provide your personal data to our distributors, resellers, or partners for the purpose of distribution, sale, or management of our products. Our distributors, resellers, or partners may communicate with you about Norton and LifeLock products or services. In addition, you may purchase our products directly from our distributor, a reseller, or an app store. Because your relationship in these cases is with that distributor, reseller, or app store, such third party will also process your personal data.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our partners: User data, Product data.

- **With Our Advertising Partners**

  We engage in personalized (or targeted) advertising in our Services or on other sites when we advertise our Services elsewhere. We may provide or share (as defined by the CCPA) your personal data, including the data about your interests in our Services, to third parties for the purposes of serving you more relevant ads about our Services. Where we provide you with interest-based ads on a site other than our own, we do not track your other activities on that site. If you click on our ads, we will know the domain you came from. For more information, please see our Cookie Statement.

  In the past 12 months since this Statement was last updated, we disclosed or shared the following categories of personal data to our advertising partners: User data, Device Data, Website data.

- **With Data Analytics Providers**

  We may provide your personal data to third parties to use the personal data in aggregate form to help us understand how our Services are being used or to understand the effectiveness of our marketing campaigns. Please see our Cookie Statement.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our data analytics partners: User data, Product data, Website data.

- **With Service Providers Processing Data on Our Behalf**

  We may use contractors and service providers to process the personal data we collect for the purposes described in this Statement, the relevant Product and Service Privacy Statements, and for business purposes such as financial auditing, data storage and security, troubleshooting and debugging, improving the functionality and usability of our websites and Services, improving and operationalizing threat intelligence and counter-threat measures, and for marketing and promoting our Services.

  We contractually require service providers to keep data confidential, and we do not allow our service providers to disclose our data or your personal data to others without our authorization, or to sell it or use it for purposes unrelated to the services they provide (e.g., their own marketing purposes). However, if you have a separate and/or independent relationship with these service providers, their privacy statements will apply to such relationships. Such service providers may include benefit brokers, your employer (for products and services offered as an employee benefit), contact centers, payment card processors, and marketing, survey, or analytics suppliers.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our service providers: User data, Product data, Website data, Third-party data.

- **With Payment Processors**

  If you pay for use of our services, you may use a third-party payment processor to take payment from you. These third parties are properly regulated and authorized to handle your payment information. However, they are independent controllers of your data with their own responsibilities.

  Your billing data is processed by the payment processor from whom you purchased the product. Your data is processed according to the relevant processor's privacy policy.

Payment Processor	Link to Privacy Policy
Google Play Store (for mobile apps)	https://policies.google.com/privacy
Apple Store (for mobile apps)	https://www.apple.com/legal/privacy/

- **With Public Authorities and Legal Proceedings**

  In certain instances, it may be necessary for us to disclose any of the personal data we collect to comply with a legal obligation, at the request of public authorities, or as otherwise required by applicable law. No personal data will be disclosed except in response to:

  - A subpoena, warrant, or other legal process issued by a court or other public authority of competent jurisdiction;
  - Discovery requests or demands as part of a civil lawsuit or similar legal process;
  - Where disclosure is required to comply with applicable laws, or necessary for us to enforce our legal rights pursuant to applicable law;
  - A request with the purpose of identifying and/or preventing credit card fraud or identity theft; or
  - Where disclosure of personal data is necessary to prevent or lessen a serious and imminent threat of bodily or other significant harm to the data subject or other individuals potentially concerned.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to public authorities: User data, Product data, Website data.

- **For Restoration Services**

  We may disclose your user data, security data, diagnostic information, and third-party data to financial institutions, financial services companies, and other third parties at your direction to provide restoration services and other Services to you.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to financial institutions: User data, product data.

- **With Third-Party Service Providers**

  If you access third-party services through our Services, these third parties may be able to collect user data, security data, diagnostic information, and third-party data about you in accordance with their own privacy policies. Some examples include:

Third-Party Login Providers
To register with us or to be able to log into our products, we offer you, in addition to our own procedure, the option to do this via the services Google, and Apple ID. For this purpose, we will redirect you to a page of the corresponding provider. You will share your login data exclusively with the provider, who in turn exchanges data with us accordingly. Please note that the service provider also receives information from us in this way.

Provider	Links
Apple	https://www.apple.com/legal/privacy/
Google	https://policies.google.com/privacy

Social Media and Internet Platforms
Our social media monitoring service uses API services from the platforms listed below. Our website and services may also contain links to those platforms. If you use the platforms listed below, your use is subject to the platforms terms of service and privacy policies available through the provided links.

Provider	Links
YouTube	Terms of Service: https://www.youtube.com/t/terms Privacy: https://policies.google.com/privacy Manage Settings: https://myaccount.google.com/permissions
Facebook	https://www.facebook.com/legal/terms/update https://www.facebook.com/privacy/policy/
Instagram	https://help.instagram.com/581066165581870?helpref=page_content https://privacycenter.instagram.com/policy

Twitter	https://twitter.com/en/privacy https://twitter.com/en/tos#update-intlTerms https://twitter.com/en/tos#update
LinkedIn	https://www.linkedin.com/legal/user-agreement https://privacy.linkedin.com/
Snapchat	https://snap.com/en-US/terms https://snap.com/en-US/terms#terms-row https://values.snap.com/privacy/privacy-center
TikTok	https://www.tiktok.com/legal/page/us/terms-of-service/en https://www.tiktok.com/legal/page/eea/terms-of-service/en https://www.tiktok.com/legal/page/row/terms-of-service/en

- **With Our Corporate Affiliates**

  We may share the information we collect with our corporate affiliates, subsidiaries, branch offices and other members of our corporate group.

  In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data third-party corporate affiliates: User data, Product data, Website data, Third-party data.

- **For Business Transfers**

  We may share the personal data we collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, acquisition, consolidation, asset sale, or initial public offering, or in the unlikely event of bankruptcy.

5. Retention and Deletion of Your Personal Data

We will keep your personal data on our systems as long as necessary to provide you with our Services, or for as long as we have another legitimate business purpose to do so, but not longer than permitted or required by law. When determining the specific retention period, we take into account various criteria, such as the type of service provided to you, the nature and length of our relationship with you, and mandatory retention periods provided by law and the relevant statute of limitations. When we no longer have an ongoing legitimate business reason to keep your personal data, your personal data will either be securely disposed of, or de-identified

through an appropriate anonymization means. Please see our Product Specific Privacy Statements for specific data retention periods.

6. Cross-Border Transfers of Personal Data Among Gen Digital and NortonLifeLock Entities and to Third-Party Vendors

We are a global company and process personal data in many countries. As part of our business, your personal data may be transferred to Gen Digital and/or its subsidiaries and affiliates in the United States, and to subsidiaries and third-party vendors of Gen Digital located worldwide, including NortonLifeLock entities. All transfers will occur in compliance with the applicable data transfer requirements laws and regulations. Transfers of your personal data within Gen Digital and/or its subsidiaries and affiliates are done pursuant to NortonLifeLock's Binding Corporate Rules.

If your personal data originates from the European Economic Area and is transferred to Gen Digital subsidiaries, affiliates, or third-party vendors engaged by Gen Digital or NortonLifeLock to process such personal data on our behalf who are located in countries that are not recognized by the European Commission as offering an adequate level of personal data protection, such transfers are covered by alternate appropriate safeguards, specifically Standard Contractual Clauses adopted by the European Commission.

If we are involved in a reorganization, merger, acquisition, or sale of our assets, your personal data may be transferred as part of that transaction.

7. How We Protect Your Personal Data

Securing personal data is an important aspect of protecting privacy. We take reasonable and appropriate physical, technical, and organizational security measures in accordance with applicable laws to protect your personal data against the risk of accidental loss, compromise, or any form of unauthorized access, disclosure, or processing. The relevant security controls are communicated throughout Gen Digital to support the secure development of Services and maintain a secure operating environment. Our security approach includes:

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.

Technical Safeguards

We implement and use information security standards, protocols, and technologies, including encryption, intrusion detection, and data loss prevention, and we monitor our systems and data centers to comply with our security policies.

Organizational Safeguards

We conduct regular company-wide as well as role-specific training and awareness programs on security and privacy. If you have any questions about the security of your personal data or the security of the site, or wish to report a potential security issue, please contact security@GenDigital.com. When reporting a potential security issue, please describe the matter

in as much detail as possible and include any information that might be helpful. If you are having problems accessing your account, please contact our Member Support Center.

8. Your Privacy Rights and Choices

You can view and update your personal data through your Norton Account or LifeLock Portal. There are a variety of data protection laws around the globe that provide privacy rights to you as our customer. Subject to applicable laws, you may have the following rights:

- **Delete**: Right to delete or erasure ("right to be forgotten") of personal data we have collected from or about you;
- **Access**: Right to know and access the personal data we have collected about you, as well as other information about our data processing practices;
- **Rectify**: Right to rectify, correct, update, or complement inaccurate or incomplete personal data we have about you;
- **Restrict**: Right to restrict the way we process your personal data;
- **Withdraw Consent**: Right to withdraw your consent to process your personal data;
- **Object**: Right to object to our processing of your personal data based on legitimate interest;
- **Object to Automated Individual Decision-Making:** Right to object to our processing of your personal data in automated individual decision-making;
- **Equal Service**: Right not to receive discriminatory treatment for the exercise of your privacy rights, subject to certain limitations;
- **Opt-Out**: Right to Opt-Out of the sale of personal data, or the Right to Opt-Out of sharing of personal data for cross contextual advertising. U.S. residents can opt out of personalized advertising as set forth here: Do Not Sell or Share My Personal Information. U.S. residents can also turn on the Global Privacy Control (GPC) to opt out of the sharing of your personal information for cross contextual advertising. Learn more at the Global Privacy Control website. You may have the right to opt out of the processing of your personal data for certain types of profiling in furtherance of decisions that produce legal or similarly significant effects. However, please note that we do not engage in such profiling.
- **Portability of Personal Data**: Right to obtain a portable copy of your personal data; and
- **Lodge a Complaint**: Right to lodge a complaint with a supervisory authority if you are not satisfied with the way we have handled your personal data, or any privacy request, or other request that you have raised with us.

To exercise any of your rights, or to raise any other questions, concerns, or complaints about our privacy practices, or about our use of your personal data and its privacy, or if you are not a customer of ours and want to know what personal data we have about you, please contact us as explained below ("Contact Us"). To exercise your rights under applicable law you can submit a request here. You may appeal any decision with regard to your privacy request by contacting us here or using the details provided in the "Contact Us" section below.

Once we receive your request, we will verify your identity and your authorization to take the actions requested, authenticating your identity at a level appropriate to the requested action. We

require you to re-authenticate before we will disclose or delete personal data. You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise your privacy rights and choices on your behalf, please contact Gen Digital Support.

Please note that there are exceptions and limitations to each of these rights, and that while any changes will be reflected in active user databases instantly or within a reasonable period of time, we may retain personal data for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so, to the extent permitted by applicable law.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on a Service may change or no longer be available to you where the processing of certain data is essential to the use of the Service or feature.

For information on the CCPA requests we have received, please see here.

9. Your Marketing Choices

You may receive marketing messages and materials from us or our affiliates.

You have choices on what communications you wish to receive from us. If you do not want to continue receiving any marketing materials from us, you have the following options:

- Click on the unsubscribe function in the communications you receive from us;
- Unsubscribe from Norton and LifeLock Marketing Offers;
- Manage your communication preferences in your Norton Account or LifeLock Portal;
- Contact our Member Services Department at 1-800-543-3562; or
- Contact our Member Services Department by regular mail at Attn.: Member Services, 60 East Rio Salado Parkway, Suite 1000, Tempe, AZ 85281.

If you choose not to receive marketing communications from us, we will honor your request.

However, we will continue to communicate with you as needed to provide the Services you are entitled to, to respond to your inquiries, or to otherwise relay transactional product or service-related messages.

Please also be aware that you may still receive information about our Services through other parties using their own mailing lists. For instance, marketing materials for our Services may also be contained in messages you receive from third parties, such as your employer, if they offer our Services as part of their employee benefits.

How to Opt-Out of Interest-Based Advertising

We partner with third parties to display advertising on our website or to manage our advertising on other sites. You may Opt-Out of many third-party ad networks, including those operated by members of the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). For more information and available choices for third-party ad networks participating in the NAI

and DAA programs, please visit their respective websites: https://optout.networkadvertising.org/ (NAI) and www.aboutads.info/choices (DAA). If you are in the European Union, you may also do so by visiting Your Online Choices (click here). Please note that if you Opt-Out, you will continue to receive generic ads not based on your interests. Opting out of these networks does not otherwise limit the collection of information described elsewhere in this Statement.

Note: If your browser is configured to reject cookies when you visit the opt-out page, or you subsequently erase your cookies, use a different computer, or change web browsers, your opt-out may no longer be effective.

10. Contact Us

Please visit our Privacy Center for data subject rights requests.

Gen Digital Inc. – Privacy Team
60 East Rio Salado Parkway, Suite 1000
Tempe, AZ 85281
Email: nll_privacy@GenDigital.com
Member Services: 1-800-543-3562

NortonLifeLock Ireland Limited –Privacy Office
Ballycoolin Business Park
Blanchardstown
Dublin 15
Ireland D15E867
Email: nll_privacy@GenDigital.com

Independent EU GDPR Data Protection Officer
Pembroke Privacy Ltd
4 Upper Pembroke Street
Dublin 2
Ireland DO2VN24
Email: DPO@GenDigital.com

11. Cookies and Third-Party Analytics

Please read our cookie and analytics notice for more information about how we use these tools.

12. Automated Individual Decision-Making and Profiling

Where Gen Digital processes network traffic data for the purpose of network and information security based on our or our customers' legitimate interest as outlined in the corresponding section of this Statement, automated decisions concerning data elements may occasionally be made. This could involve assigning relative cybersecurity reputation scores to IP addresses and URLs based on objective cyber-threat indicators measured by our and our partners' cyber-threat detection engines. Such indicators may be, for instance, the determination that malicious or otherwise harmful contents are hosted at a given URL or are coming from a given IP address. Such automatically assigned reputation scores may be leveraged by you, by Gen Digital, by our partners, and by other customers to detect, block, and mitigate the identified cyber threats. They

could therefore result in our Services blocking network traffic coming from or going to such URLs and IP addresses. This processing is intended only to protect you, Gen Digital, our partners, and our other customers from cyber threats. If you consider that such automated processing is unduly affecting you in a significant way, please contact us as explained above ("Contact Us") to raise your concerns or exercise your right to object and to seek our help in finding a satisfactory solution.

13. Children's Privacy

Our websites are not directed to, nor do we knowingly collect data from, minors (as defined by applicable law) except where explicitly described otherwise in the privacy notices of Services designed specifically for purposes such as to assist you by providing child online protection features. In such cases, we will only collect, and process personal data related to any child under 13 years of age that you choose to disclose to us or otherwise instruct us to collect and process. We also do not sell or share personal information of consumers under 16 years of age. Please refer to the Product Specific Privacy Statements for additional information.

14. Changes to this Statement

We reserve the right to revise or modify this Statement. In addition, we may update this Privacy Statement to reflect changes to our personal data processing practices. If we make any material changes in the way we collect, process, use and/or disclose your personal data previously collected from you through our Services, we will attempt to notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. In the case of a material change to our personal data processing practices, any such change will only apply on a going-forward basis. We will not process the personal data currently in our possession in a materially different way without your prior consent. We encourage you to periodically review this page for the latest information on our privacy practices.

15. Links to Other Websites

Our websites may contain links to other websites owned or operated by other companies. If you visit any linked websites, please review their privacy statements carefully. We are not responsible for the content or privacy practices of websites that are owned by those third parties. Our websites may also link to co-branded websites that are maintained by Gen Digital and one or more of our business partners who are collecting your personal data pursuant to their own privacy practices. Please review the applicable privacy statements on any co-branded site you visit, as they may differ from ours.

16. Disclaimer

This Privacy Statement does not apply to Gen Digital affiliates: (1) Avira Operations GmbH & Co. KG., including its related entities; (2) ReputationDefender LLC; (3) Avast Software sro, including its related entities. These entities maintain separate privacy statements which can be found on their respective websites.

LAST UPDATED: July 13, 2023