PC Peripherals & GDPR Compliance

Company	**PC Peripherals**
	67A Heather Road,
	Sandyford Industrial Estate,
	Dublin 18.
Phone	**01 2917900**
Data Protection Officer (DPO)	**Martin Byrne**
DPO Email Address	**dpo@pcp.ie**
DPO Contact Phone Numbers	**01 2917910 / 087 2606805**

GDPR Compliance / Document Control

Version	Date Issued	Summary of Changes
0.1	23/10/ 2017	Initial Draft
0.2	09/01/ 2018	Appointed DPO / Staff Q&A
0.3	08/02/2018	Incorporated Checklist / Staff Training
0.4	14/03/2018	Website Security address and BOYD/Mobile device lock down
0.5	04/04/2017	3rd party review & finalise
1.0	23/05/2018	Published

Document Contents;

PC Peripherals/GDPR Compliance Flow Chart

PC Peripherals Privacy Policy 2018

The General Data Protection Regulation (GDPR) will in force from the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

GDPR Executive Summary

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access but differs from it in many ways. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.
Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies. In this regard, WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form.

As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.

The opinion also helps data controllers to clearly understand their respective obligations and recommends best practices and tools that support compliance with the right to data

portability. Finally, the opinion recommends that industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

PC Peripherals PRIVACY STATEMENT

PC Peripherals is committed to protecting the privacy of your information in accordance with the principles set out in the GDPR (25th May 2018). This policy document explains how we use personal information we collect about you when you use our services or get in contact with us.

PC Peripherals / GDPR Action Chart

Personal Privacy	Controls and Notifications	Transparent Policies	IT and Training
Individuals have the right to: Get access their personal data Correct errors in their personal data Erase their personal data Object to processing of their personal data Export personal data	**PCP will undertake to:** Protect personal data using appropriate security Notify authorities of personal data breaches Obtain appropriate consents for processing data Keep records detailing data processing	**PCP is required to:** Provide clear notice of data collection Outline processing purposes and use cases Define data retention and deletion policies	**PCP will undertake to:** Train privacy personnel and employees Audit and update data policies Employ a Data Protection Officer (if required) Create and manage compliant vendor contracts

Privacy by Design

PC Peripherals will implement 'Privacy by Design' by undertaking the processing of personal data with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems. The IT department, or any department that processes personal data, will ensure that privacy is built in to a system during the whole life cycle of the system or process.

PC Peripherals will implement Privacy by Default by ensuring when a product or service is made available to our clients, strict privacy settings should apply by default, In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service.

GDPR Commitment

We at PC Peripherals are committed to the protection of all of our customers' data and the lawful use and processing of that data. Historically PC Peripherals have been to the fore with Data Protection however with the arrival of the GDPR, we have further updated our procedures to ensure compliance with all GDPR-specific requirements, this enhanced certification/compliance provides contractual safeguards to our customers for the processing of the personal data by PC Peripherals, enabling these customers to be compliant with the GDPR.

Section 1 – What do we do with your information?

When you purchase a product or service from PC Peripherals, as part of the buying and selling process, we collect the personal information you give us such as your name, address and email address. **We do not store any personal banking or credit card details.**

When you browse our store online, we also automatically receive your computer's internet protocol (IP) address in order to provide us with information that helps us learn about your browser and operating system.

Email marketing (if applicable): With your permission, we may send you emails about our store, new products and other updates – you have to opt-in / sign up to receive this information.

We also collect information about your use of our websites and how you arrived at our website in the first place. This can include what links or adverts of ours you viewed or clicked on to reach us, or any search terms you have used. We can also see which pages of our websites you have viewed and for how long. All this information helps tell us what content is popular with our customers so we can improve our services and products.

Section 2 - Consent

How do you get my consent?

When you provide us with personal information to complete a transaction, place an order, arrange for a delivery or return a purchase, we take it as a commitment that you consent to our collecting it and using it for that specific reason only.

If we ask for your personal information for a secondary reason, like marketing, we will either ask you directly for your expressed consent, or provide you with an opportunity to say no.

How do I withdraw my consent?

If after you opt-in, you change your mind, you may withdraw your consent for us to contact you, for the continued collection, use or disclosure of your information, at any time, by

contacting us at reception@pcp.ie or mailing us at: FAO – DPO, PC Peripherals, 67A Heather Rd, Sandyford Industrial Estate, Dublin 18, Ireland.

Section 3 - Disclosure

We may disclose your personal information if we are required by law to do so or if you violate our Terms of Service.

Section 4 – Third Party Services

In general, the third-party providers used by us will only collect, use and disclose your information to the extent necessary to allow them to perform the services they provide to us.

However, certain third-party service providers, such as payment gateways and other payment transaction processors, have their own privacy policies in respect to the information we are required to provide to them for your purchase-related transactions.

For these providers, we recommend that you read their privacy policies so you can understand the manner in which your personal information will be handled by these providers.

In particular, remember that certain providers may be located in or have facilities that are located in a different jurisdiction than either you or us. So if you elect to proceed with a transaction that involves the services of a third-party service provider, then your information may become subject to the laws of the jurisdiction(s) in which that service provider or its facilities are located.

As an example, if you are located in Canada and your transaction is processed by a payment gateway located in the United States, then your personal information used in completing that transaction may be subject to disclosure under United States legislation, including the Patriot Act.

Once you leave our store's website or are redirected to a third-party website or application, you are no longer governed by this Privacy Policy or our website's Terms of Service.

Web-Links

When you click on links on our store, they may direct you away from our site. We are not responsible for the privacy practices of other sites and encourage you to read their privacy statements.

Section 5 - Security

To protect your personal information, we take reasonable precautions and follow industry best practices to make sure it is not inappropriately lost, misused, accessed, disclosed, altered or destroyed.

If you provide us with your credit card information, the information is encrypted using secure socket layer technology (SSL) and stored with a AES-256 encryption. Although no method of transmission over the Internet or electronic storage is 100% secure, we follow all PCI-DSS requirements and implement additional generally accepted industry standards.

Cookies

Here is a list of cookies that we use. We've listed them here so you can choose if you want to opt-out of cookies or not.

_session_id, unique token, sessional, Allows Shopify to store information about your session (referrer, landing page, etc).

_shopify_visit, no data held, Persistent for 30 minutes from the last visit, Used by our website provider's internal stats tracker to record the number of visits

_shopify_uniq, no data held, expires midnight (relative to the visitor) of the next day, Counts the number of visits to a store by a single customer.

cart, unique token, persistent for 2 weeks, Stores information about the contents of your cart.

_secure_session_id, unique token, sessional

storefront_digest, unique token, indefinite If the shop has a password, this is used to determine if the current visitor has access.

Section 6 – Age of Consent

By using this site, you represent that you are at least the age of majority in your state or province of residence, or that you are the age of majority in your state or province of residence and you have given us your consent to allow any of your minor dependents to use this site.

Section 7 – Changes to this Privacy Policy Statement

We reserve the right to modify this privacy policy at any time, so please review it frequently. Changes and clarifications will take effect immediately upon their posting on the website. If we make material changes to this policy, we will notify you here that it has been updated, so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we use and/or disclose it.

If our store is acquired or merged with another company, your information may be transferred to the new owners so that we may continue to sell products to you, again this information will be relayed at that time.

GDPR Compliance / PC Peripherals (In General)

PC Peripherals GDPR Compliance policy provides for the consistent application of security principles throughout the company. After Implementation, it is a reference guide when matters of security arise. The policy ensures management's commitment to maintaining a secure Network, which allows the IT Staff to do a more effective job of securing the company's information assets & reduces the risk of a damaging security incident. And in the event of a Security incident the Incident Response Policy is deployed. The individual security policies below are part of our overall Security Policy.

- Acceptable Use Policy
- Authentication Policy
- Backup Policy
- Confidential Data Policy
- Data Classification Policy
- Encryption Policy
- Email Policy
- Guest Access Policy
- Incident Response Policy
- Mobile Device Policy
- Network Access Policy
- Network Security policy
- Outsourcing Policy
- Password Policy
- Physical Security policy
- Remote Access Policy
- Website Compliance

Information We Collect;

PC Peripherals have assessed the risks involved in processing personal data and have put measures in place to mitigate against date leakage.

You may choose to give us information about you by filling in forms on our site such as the Contact Us Form or by corresponding with us by phone, e-mail or otherwise. PC Peripherals only asks you to disclose as much information as is necessary to provide you with information requested by you or to submit a question/suggestion/comment in relation to our website.

We may also collect details of your visits to our site (including, but not limited to, traffic data, location data, weblogs and other communication data), and the resources that you access. When you access our website, your computer's browser provides us with information such as your IP address, browser type, access time and referring URL, which is

collected and used to compile statistical data on the use of our website. This information may be used to help us to improve our site and the services we offer.

PC Peripherals proposes to request as little data as possible;

The GDPR states that organisations shouldn't process or retain extraneous personal data. That means data should be collected for a specific purpose, used only for that purpose and retained for only as long as it meets that purpose. PC Peripherals will typically collect company/individuals' names and contact information at the very least, specifically for the task at hand.

Make the terms and conditions clear;

PC Peripherals endeavour to making all consent mechanisms to be as easy as possible to use and kept separate from other terms and conditions, and are presented in a clear, concise and easily understandable.

Make it easy to withdraw;

All Consent requests will be presented in a manner as to make it as easy for individuals to withdraw their consent as it is for them to give it.

Use a double opt-in mechanism;

PC Peripherals engage a double opt-in mechanism that guarantees that individuals don't give their consent by accident. The first step involves a regular consent form. Once the individual has completed it, they'll receive an email with an attached link that they need to click on to verify their registration.

Double opt-in consent doesn't involve too much extra work for either the organisation or the individual, many people are already familiar with it as it's often used to activate new accounts and it makes sure that those who provide their consent are genuinely interested in the service on offer.

How Your Information is Used;

Where you submit your personal information to us, it will only be used for the stated purpose and any reasonably incidental purposes.

Such information will only be used by us;

For the purposes for which it was provided by you and any reasonably incidental purposes including providing you with the information that you request from us.

For marketing and administration purposes – with an opt-out option.

For analyses purposes including ensuring that content from our site is presented in the most effective manner for you and for your computer.

PC Peripherals undertakes not to sell or rent to any third party whatsoever any personally identifiable information about you.

Your Rights;

You should ensure that the information we collect and hold in relation to you is accurate and kept up to date. If you would like to review the information we have collected - you may request that information at any time.

You also have the right to have the information erased if we do not have a legitimate reason for retaining same. We will accede to any such valid requests within 40 calendar days of the receipt of a valid request in writing.

All information collected will be made available in a commonly used and machine readable format.

Retention procedures are in place to ensure that data is kept for no longer than for what it was originally collected for.

All data collected are covered by procedures to eliminate unnecessary and unregulated duplication.

Our website may, from time to time, contain links to and from the websites of our Members, partner networks, advertisers, event organisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Governing Law and Jurisdiction;

This legal notice and all issues regarding the www.pcp.ie website are governed exclusively by Irish law and are subject to the exclusive jurisdiction of the Irish courts.

General;

Delay or failure on our part in enforcing any of our rights shall not constitute a waiver by us of our rights and remedies. If any part of this GDPR Compliance / Privacy Statement is held to be invalid or unenforceable, the validity or enforceability of the remainder will not be affected.

GDPR Key Developments:

- **Appointment of a Data Protection Officer (DPO)**: PC Peripherals have appointed a DPO to manage GDPR Compliance and to ensure we are aware of the latest privacy changes to maintain best practices and protect customer data.
- **Enhanced privacy and security awareness program**: A new comprehensive, company-wide privacy and security training portal to augment our GDPR obligations. Every PC Peripherals employee, regardless of whether they access to customer data, will receive important and up-to-date training on data privacy and security.

- **Introduction of New GDPR features**: To ensure that our Technical Department practices follow the GDPR rules with regard to Network Lockdown / service / image deployment / installation / BOYD / Mobile devices / Storage and implementation.
- **Introduction of New Marketing rules** - We want our customers to receive the information that they want & when they want it, the selection process will empower the client to ensure they are getting the latest product and company updates from us, and not getting information you don't want.
- **Centralised privacy & compliance information**: We will endeavour to provide easy, centralised access to relevant compliance and security documents, including updates on our GDPR efforts. The privacy landscape is changing fast and we take very seriously the immense responsibility of caring for our customers' data.

PC Peripherals Company Policy / GDPR Enforcement

Data Protection

PC Peripherals are fully registered with the Data Protection Commissioner as Data users and Data controllers.

Staff Training;

Comprehensive staff training to make each employee aware of PC Peripherals obligations under the GDPR directive.

Network;

Comprehensive Gateway Security Suite - High-performance security engine, Intrusion prevention, Advanced IPSec and SSL VPN, Gateway anti-virus and anti-spyware, Streamlined GUI and advanced management, Content/URL filtering, Wireless network security. 90day change of password policy.

Trend Micro Worry Free - Small Business Cloud-Based Security;

Trend Micro Worry Free Protects Against – Viruses, Hackers, Spyware, Dangerous Websites & Data theft. It offers Threat Protection in the form of - High-fidelity machine learning (pre-execution and runtime), Behavioural analysis (against scripts, injection, ransomware, memory, and browser attacks), File reputation, Web reputation, URL filtering, Device control, Firewall, Device control & Application control.

Office 365/Exchange;

The Data Loss Prevention Policy (DLP) policy in the Office 365 Security & Compliance Center, allows PC Peripherals to monitor, and automatically protect sensitive information across Office 365/Exchange.

Mobile/BOYD Devices;

Pin & Password Access / Auto-lock after 1 minute / Device remotely wiped if it is stolen, compromised, breached. 90day change of password staff policy.

Company Laptops & PCs;

BitLocker & Deslock Encryption / System & HDD password protected.

System Imaging ;

Secure 2 Step authentication for access to image server – any related HDDs/USB Keys/Data disks are formatted once the image has been stored on the image server.

USB Storage/External Hard Drive;

AES 256Bit Encryption and key pad USB HDDs for portable data storage.

Data Privacy Agreements;

PC Peripherals will enter into any Data Privacy Agreements with our clients if required (under legal agreement).

Penetration/Vulnerability Tests;

PC Peripherals will run regular Penetration/Vulnerability Tests on our internal/external network to ensure the highest GDPR standards are always in place.

Printing;

Secure network PIN printing practices with recording of employee and file printed.

Website/Newsletters;

Opt in/opt out options available to potential subscribers.

Paper Disposal / Shredding

GDPR compliant 3rd Party contractor shredding facility.

Partner Compliance;

Complete file of GDPR compliance statements from each supplier.

Courier/Delivery Compliance;

Complete file of GDPR compliance statements from each service provider

Obsolete Equipment Disposal & Destruction;

Recycling partner – www.kavanaghrecycling.ie - certified WEEE Recycling and Secure Data Destruction facility.

Obsolete Equipment Storage;

In the event of PC Peripherals been contracted to store obsolete equipment for a period of time – all related PC hardware is stored on site in secured storage enclosures.

Staff Vehicles;

Vehicle fitted with alarm and immobilisers, designated parking with CCTV footage if available. No-visible hardware policy adopted.

Secure Building;

Monitored alarm system / complete shutter lock window & door protection / department lockdown and secure /fireproof image retention area.

Questions & Contact Information

If you would like to: access, correct, amend or delete any personal information we have about you, register a complaint, or simply want more information contact our Data Protection Officer at;

Email	:	dpo@pcp.ie
Phone	:	01 291 7900
FAX	:	01 291 7999
Address	:	PC Peripherals, 67A Heather Rd, Sandyford Industrial Estate, Dublin 18.