

1. Scope of application and contents of these Terms of Use for IT Systems

These Terms of Use for IT Systems apply to all employees who are employed by the PAYBACK GROUP or work for it under the terms of a staff leasing agreement.

When you access the PAYBACK GROUP's IT systems (i.e. all our hardware and software, including PCs, laptops, routers, operating systems, browsers and communications software, and any services we provide, including cloud services and cloud storage), you have to comply with the following regulations.

The Terms of Use for IT Systems set out in this document replace all prior versions of this document. Where the handling and use of special IT systems are subject to their own terms of use, those terms of use take precedence. Unless otherwise stipulated, they are nevertheless supplemented by the Terms of Use for IT Systems set out in this document.

2. Personal use

You may use your client devices (e.g. laptop, smartphone, keyboard, mouse, and headset) for personal use, within the limits set out in this document, where you have given your separate consent with respect to data protection and the secrecy of telecommunications. You can give and revoke your consent in the personnel system, as described [here](https://toolbox.loyaltypartner.com/index.php?id=110&L=1) in the toolbox (<https://toolbox.loyaltypartner.com/index.php?id=110&L=1>).

Since there is no technical distinction between the business and personal use of our IT systems, personal use is only possible and permitted from a legal perspective if you agree that any personal use, and any personal data generated in that context, will be treated like any business use from a technical or legal perspective.

We have the right to revoke our permission with respect to personal use at any time. Permission with respect to personal use is granted at our sole discretion and does not give rise to a legal right to personal use, even where permission is granted repeatedly and without the express reservation of voluntariness. If you do not agree to this equal treatment and do not give your consent or later revoke your consent, personal use is not possible or permitted.

Once you have given your consent, you may also use business IT systems for personal use outside of working hours. However, during working hours, you may only use the systems for personal use in personal emergencies or in urgent exceptional situations which cannot be postponed, and only within reasonable limits.

<i>Subject</i>	<i>Personal use</i>
Laptop	Permitted*, **
Smartphone	Permitted*
Internet	Permitted*
OneDrive	Not permitted
Email (business email address and business email system)	Not permitted
Installation or execution of applications that have not been approved	Not permitted
Central IT systems, cloud services and cloud storage, other IT systems	Not permitted

* Within the limits described in the Terms of Use for IT Systems

** In the user directory (Windows: C:\Users\<Your login name>\Private files, Mac: /Users/<Your login name>/Private files, Fedora: /home/loyaltypartner.com/<Your login name>/Private files)

Important note: when saving personal documents, you need to create a folder named "Private files" and you must classify the documents using the label "No-Business" (for further information see Section 3. Data classification).

3. Data classification

We classify our data and information in specific categories. Different rules apply depending on the category. Before you use data or information, you need to determine the appropriate category and comply with the associated rules.

Further binding rules and details regarding this subject are available in the following documents: "LP-IS02.01 Information Ownership and Classification Standard" and "PLP-IS02.01.01 Information Classification, Labeling and Handling Reference Guide" (in the PAYBACK Security Sharepoint or directly here <https://loyaltypartnergroup.sharepoint.com/:b:/r/sites/PAYBACKSecurity/Policies/PLP-IS02.01.01%20Information%20Classification,%20Labeling%20and%20Handling%20Reference%20Guide.pdf?csf=1&web=1&e=IUXKW1>).

4. Data storage

Storage location	Private data	Business data
Storage on personal devices	Permitted	Not permitted
Storage on business client devices	Permitted*	Permitted**
Storage on a central IT system	Not permitted	Permitted
Storage on OneDrive	Not permitted	Permitted***

* In a folder named as described in Section 2 and within the limits described in these Terms of Use for IT Systems

** Data is only backed up from network drives, not on client devices

*** When employees leave the company, business data must be stored in a central IT system outside of OneDrive

Business data may only be stored in the PAYBACK GROUP's IT systems. Where data has to be temporarily stored on client devices, this data must also be regularly (i.e. not less than once a week) transferred to a central IT system other than OneDrive.

Where you save personal data on business devices, please note that it will be erased by us when the devices are returned. It will not be possible to restore such data afterwards. We therefore recommend that you save your personal data on a different storage medium before returning the devices.

5. Cloud services and cloud storage

You may only use the cloud services and cloud storage that are provided by the PAYBACK GROUP and any service providers approved by it.

6. Removable storage media

Only authorized removable storage devices (e.g. USB memory, memory cards, etc.) may be used for work-related purposes. Sensitive information should generally not be stored on removable storage devices. If this is necessary, the data must be stored in encrypted form. You can find instructions on how to do this here:

<https://toolbox.loyaltypartner.com/index.php?id=162>.

Business data must not be stored on private removable storage devices.

7. AI based cloud systems

The use of AI systems for business purposes is generally restricted. Under no circumstances may personal data, sensitive business or customer data, passwords, legal documents or business agreements be processed. Only information classified as 'LP-Public' may be processed. The result, which originates from an AI system, must be clearly labelled for further use (e.g. ...was generated by M365 Copilot).

The use of generative AI systems such as Chat GPT is generally prohibited, as they do not offer any significant protection and we do not have a contractual relationship that could provide any guarantees regarding the use of our data. Instead, the company has enabled M365 Copilot and Bing Copilot respectively, both of which are powered by Chat GPT and are equally powerful. They also offer a degree of protection covered by the contract with Microsoft.

8. General rules

Our IT systems may not, under any circumstances, be used in a way or for purposes that violate the law, infringe our rights and/or those of third parties, compromise or breach the confidentiality of data or information associated with us, disrupt our operations, impair the availability of our IT systems, violate internal regulations including the Terms of Use for IT Systems set out in this document, damage our reputation, or cause us to incur additional expenses.

The following use of our IT systems in particular is not permitted:

- Visiting websites the use of which we have prohibited because there is a strong possibility that they contain malware, e.g. viruses or Trojans
- Viewing, creating, downloading, saving or forwarding illegal or offensive content; accessing websites with illegal content (e.g. libellous, obscene, racist or sexist content or content that glorifies violence)
- Downloading and installing software from the Internet (e.g. MP3, programs, games, drivers); cf. Section 11.

Confidential information (LP Secret and LP Restricted including sub-labels) must be encrypted before being exchanged. Documents that are classified as such are encrypted automatically.

9. Rules for using email

- Emails containing confidential information or attachments (LP Secret and LP Restricted) must be designated as such.
- Confidential information (LP Secret and LP Restricted) must be encrypted if it is sent to external recipients. Detailed guidance on this is available in the PAYBACK Security Sharepoint (<https://loyaltypartnergroup.sharepoint.com/sites/PAYBACKSecurity/SitePages/E-mail-&-Phishing.aspx>).
- Your personal emails must be filed in a folder named "Personal email" in the email client. You need to create this folder. This does not refer to private emails (see above: our email system must not be used for personal use), but business emails that only concern you personally, e.g. your business correspondence with your supervisor.
- In general, all emails received and sent through our business email system are stored in an archiving system. The purpose of that system is not to make emails available again to employees in day-to-day operations, but to comply with statutory retention periods. Consequently, you cannot access those emails.
- Every email sent and received through our email system is automatically screened for malware, advertising and attempts at fraud. Emails that meet specific, regularly adjusted criteria are blocked automatically and will not be delivered to you. You will be notified of emails that are merely classified as suspicious. You can approve these using the self-service function. In general, emails may only be approved if they contain business-related data or information that is undamaged and not compromising.

10. Handling of our IT devices

- Avoid the loss (e.g. theft) of your IT devices by acting appropriately. Further tips are available [here](https://toolbox.loyaltypartner.com/index.php?id=137&L=1) (<https://toolbox.loyaltypartner.com/index.php?id=137&L=1>).
- The loss of any kind of IT device must be reported to the IT department (IT-Nutzungsbedingungen@loyaltypartner.com) and your supervisors without undue delay.
- Physical changes to our IT devices may only be made by the PAYBACK GROUP's IT department; you are not authorised to make any such changes yourself.
- Our devices may not be exchanged with those of external contractors or internal staff. Changes to the assignment of persons to our devices may only be made by our IT department.
- Only PAYBACK GROUP devices approved by our IT department may be used in the network.
- Devices must be returned to the IT department within 5 working days as soon as they are no longer needed (e.g. because the contract has been terminated or the business purpose no longer exists).

11. Software use

For security and licensing reasons, only software, programs, and libraries approved by the PAYBACK GROUP may be used in our IT systems. Approved software and programs are available through automated software distribution. This means you are forbidden to download, install, execute, or use any software unless our IT department expressly allows you to do so. This applies regardless of the authorization level assigned to you in your device's operating system. This prohibition also applies to programs that do not have to be installed separately, e.g. browser extensions. You may not modify or delete software, programs, or libraries; such tasks are the responsibility of our IT department.

Any duplication (e.g. copying or installation on other devices) of the software provided by us is strictly prohibited. The same applies to the transmission of this software and its installation on non-company hardware.

12. Monitoring compliance with the Terms of Use for IT Systems / personal data and data protection

Your use of our IT systems generates various types of your personal data which we process to be able to manage the related technical processes, for example to carry out the login process, establish an Internet connection, or send an email. More detailed information on what personal data we process and the related purpose is available in the Privacy Notice for Employees. This Notice is available in the toolbox (<https://toolbox.loyaltypartner.com/index.php?id=1018&L=1> under "Data protection (GDPR)"). Your data will also be used for purposes of data protection monitoring, IT security, data backups, and to ensure proper operation. This also includes a review as to whether our rules for the use of IT systems, in particular in accordance with these Terms of Use for IT Systems, are complied with.

This data is only accessed and used by individuals with the appropriate permissions. Please note that any violation of the rules set out in our Terms of Use for IT Systems may result in consequences under labour law.

Some IT systems are subject to special privacy notices. You will be separately advised of their application when you use those systems.

13. Rules when leaving the company

When you leave our company, whether it is temporarily (e.g. maternal leave, parental leave, treatment at a health resort (German: Kur)) or permanently (e.g. termination of employment, retirement), you need to use this [checklist](https://toolbox.loyaltypartner.com/index.php?id=136) (<https://toolbox.loyaltypartner.com/index.php?id=136>) to ensure that all personal and private data has been deleted. The foregoing obligations do not apply to files, data, or emails that you cannot access any more because they have already been archived automatically.

All IT devices made available to you for use must be given or sent back to the IT department on the last day of your employment with us. You must ensure that all operationally relevant data is stored on a central IT system other than OneDrive.

14. Contact

IT technical support:

 +49 (0) 89 997 41 – 690

 IT-Nutzungsbedingungen@loyaltypartner.com

15. Note concerning the scope of application

The following companies are part of the PAYBACK GROUP: Loyalty Partner GmbH, Loyalty Partner Kundenbindungssysteme GmbH, Loyalty Partner Polska Sp. z o.o., Loyalty Partner Polska Sp. z o.o. Sp. komandytowa, Loyalty Partner Singapore Pte Ltd., Loyalty Partner Solutions GmbH, Loyalty Solutions & Research Pte Ltd, PAYBACK GmbH, and PAYBACK Austria GmbH