cloudflight

IT Policy

1.2.2022, Version 1.1

Table of content

1. General

1.1 Objectives

This policy of Cloudflight GmbH and all its affiliated companies, hereinafter referred to as "**Cloudflight**", applies to all types of provision of internal information and communication services as well as internet access, in particular in the company, in the home office and in the context of mobile use (e.g. via notebook, tablet, smartphone). This policy also contains the measures taken by cloudflight to protect (personal) data from unauthorized access by third parties or unauthorized employees[1].

Specifically, it includes:

- Internet access as well as all other information and communication services, in particular email and Confluence or similar documentation services, Chat and Instant messaging, video conferencing, etc. and its management ("**communication technologies**") as well as

- the IT infrastructure and all devices provided by Cloudflight, such as personal computers (PCs), laptops, smartphones, tablets, tokens, all security chips, access cards, etc., as well as the software installed on them that is required for official purposes ("**IT Assets**").

The objectives of the policy are primarily:

- to limit risks as far as reasonably possible through the use of electronic data processing, in particular of the Internet and communication channels from and to the outside for operational as well as personal data of Cloudflight and third parties worthy of protection,

- to make conditions of use as well as control measures as transparent as possible towards the people affected by this policy.

1.2 Scope of Application

This policy applies to Cloudflight and applies personally to all employees of Cloudflight. This includes all regular employees, working students, trainees, and managers. For external employees, this policy applies as far as reasonable.

1.3 Effectiveness

The effectiveness of this policy is continuously validated using suitable technical and organisational measures and deficits are settled immediately.

2. Terms of use for the communication technologies

2.1 General

The communication technologies are generally provided by Cloudflight for business purposes and may only be used for business purposes, unless exceptions are provided for in the following.

[1] For reasons of better readability, only the masculine form is used for persons, whereby any gender is always included in the addressing (m/f/d).

In any case, a use which impairs the interests of Cloudflight has to be refrained from. An impairment of interests is especially given, if the public reputation or the security of Cloudflight's IT-systems are impaired, Cloudflight suffers other disadvantages, condemn legal regulations, or instructions of Cloudflight are violated. Accordingly, these are in particular, but not conclusively:

- any disclosure or endangerment of company or business secrets, personal data or other information of Cloudflight, which are marked as confidential or where confidentiality results from the nature of the information;

- deliberately retrieving, offering, distributing or storing content that violates personal rights, copyright, data protection law or criminal law, in particular the unauthorized downloading or offering of music, films, software or other content protected by copyright;

- deliberately downloading, offering, distributing or storing content that damages reputation, is insulting, defamatory, discriminatory, inhuman, racist, anti-constitutional, sexist, glorifies violence or pornographic;

- deliberately retrieving, offering, distributing or storing computer viruses or other malware as well as other activities directed against the security of IT systems;

- retrieval of contents which are subject to charges for Cloudflight, as far as this is not done for operational purposes; or

- the use of communication technologies for non-operational commercial or other business purposes.

2.2 Private use

A claim for private use of provided communication technologies does not exist. If and as far as a private use is granted by Cloudflight in the following, this is done voluntarily and is at the sole discretion of Cloudflight.

Availability and faultlessness of the internet access are not owed; disturbances and restrictions at any time, especially blocking of certain services and restriction of the available bandwidth, are reserved. Cloudflight is entitled to terminate or revoke the permission at any time at its own discretion. This applies in particular (but not conclusively) if employees violate this agreement or facts give reason to suspect this.

In the event and as long as the employee has voluntarily consented to the control of his usage in accordance with the "**Consent to Private Use of Company Internet Access**", Cloudflight allows the employee the private use of the internet access, as far as the proper performance of the work and other duties assigned to the employee are not impaired.

The consent can be revoked accordingly at any time with effect for the future. This shall not affect any statutory permissions. The revocation is excluded insofar as it relates to data and information that arose prior to the revocation. This allows Cloudflight

to carry out controls in particular even after a revocation and to draw consequences in case of violations, as far as the period before the revocation is concerned. The exclusion of the right of revocation does not apply, as far as legitimate interests of the employee oppose it, even under consideration of the legitimate interests of Cloudflight.

The permission for private use of the Internet access according to previous statements above ends upon receipt of the termination or revocation notice from Cloudflight by the employee, if the employee revokes his consent in accordance with "**Consent to Private Use of Company Internet Access**" or if the consent in accordance with "**Consent to Private Use of Company Internet Access**" becomes invalid (for example, due to a change in the legal situation) and the employee becomes aware of this, whichever occurs earlier.

Communication technologies registered via a company account of one of the Cloudflight companies, in particular e-mail in external use under the business e-mail addresses, may only be used for business purposes. This applies to outgoing messages as well as incoming messages (e.g. using the company e-mail address for private orders).

2.3 Company communication via Email

For business E-Mail communication, only the technical facilities provided by Cloudflight and respectively set up company accounts of the Cloudflight companies may be used. This also applies to accounts provided by customers throughout the lifetime of a project.

The redirection, forwarding or storing of business information, messages or files to private accounts or to unauthorized, private data carriers or storage services (in particular private cloud services) is not permitted.

If messages with private content are received on the company account of the communication technologies, the sender must be informed that the company account may only be used for company purposes and therefore no further private messages should be sent to the company address. If the message contains exclusively private content, it must be deleted immediately by the recipient; it may be forwarded to a private account of the recipient beforehand. This forwarded message must be deleted immediately as well.

In the context of substitution or other operational tasks (in particular system administration, controls, submission obligations), it cannot be ruled out that messages of a private nature are taken note of by persons other than the respective owner of the account. In this case, the content must be kept confidential, unless there are special permissions outside of this agreement (e.g. legal permission to prosecute criminal offenses). Within the scope of system administration, the necessity of accessing third-party messages must always be checked separately.

Incoming and outgoing electronic messages are automatically archived by Cloudflight for the duration of legal retention obligations (cf. § 147 AO, § 257 HGB) and, if applicable, operational necessities, especially in the context of legal disputes. Backup copies of Email access are also made on a regular basis. For technical reasons, no distinction is made between messages of a business and private nature. It is not possible to selectively delete certain messages, especially private ones. It is therefore also in the interest of the employee's personal rights to comply with the ban on private use of Email access.

Cloudflight may be obliged by domestic and foreign laws to access messages and files of the employee, to evaluate them and to pass them on to domestic and foreign authorities. This agreement does not affect any rights and obligations of Cloudflight in this respect.

2.4 Absence, Leaving

If an employee does not designate a substitute or if no designated substitute is present when the employee is absent, the team or project management or, in case of doubt, the management shall substitute or designate one or more substitutes and inform the employee of this if possible. The designation shall only be made if the employee and all representatives are absent for at least two days or in case of imminent danger which must be documented by management in writing.

Substitutes in accordance with the previous paragraph may only access the employee's company accounts, such as e-mail access, during the absence or after the employee has left the company. Substitutes may not open messages that are recognizably private in nature. If the private nature of the message becomes apparent only after it has been opened, the message must be closed immediately; the contents must be kept confidential. However, senders of private messages must also be informed by the substitute that company accounts may only be used for company purposes and that no further private messages should therefore be sent to the company address.

Irrespective of the restrictions of the previous paragraph, Cloudflight and persons commissioned by Cloudflight are entitled, within the scope of proportionality, to read access to all company messages of the employee's company accounts at any time, as far as this serves company purposes.

After the employee's departure (including death), Cloudflight may maintain personal company accounts for up to three months and grant access to a substitute or forward incoming messages to the substitute. All senders are to be informed by the substitute or automatically that the employee can no longer be reached at this address and, in the case of company messages, who is the new company contact.

On the day of exemption, all access rights of the employee to communication technology are revoked.

2.5 Filters, Logging, Control

Company accounts such as e-mail access serve exclusively, internet access primarily for company use. Therefore, Cloudflight is entitled to restrict the use of e-mail and internet access by using filter systems at its own discretion. For example, but not exclusively, blocking of certain addresses (e.g. domains, URLs), services/protocols (e.g. file sharing, streaming) or ports, the use of content-based filter systems (e.g. blocking of certain keywords or file types) as well as the use of spam and virus filters may be considered. For technical reasons, the use of such systems is in many cases associated with an automatic analysis of the content of the communication as well.

Cloudflight is also entitled to refuse the acceptance of messages from individual senders, groups of senders or domains, especially if it is to be assumed that it is an unauthorized private use of the e-mail access or other unwanted messages.

The use of communication technologies is logged and stored. For technical reasons, it is not possible to distinguish between private and business use. Logging takes place with date/time, service used (e.g. e-mail, HTTP), sender and recipient data (e.g. IP addresses, names of computers, e-mail addresses), user data if applicable (e.g. user name when sending e-mail or using a proxy server), URLs of the websites called up if applicable, technical status codes and volume of data transferred. The logs are anonymized after seven days with regard to the IP address and the name of the company computer calling up a website or receiving or sending a message, as well as with regard to the company address acting as recipient or sender, unless longer storage is required in individual cases for reasons of data and system security or for error identification and correction, or personal logging is required in accordance with the “Log analysis” process description as per the appendix “**Logging and analysis procedures**”.

3. Terms of use for the IT assets

3.1 General principles

The use of private hardware and software for business purposes without the consent of Cloudflight is not permitted, because Cloudflight is not able to ensure the required IT and data security under these circumstances.

3.2 Hardware

Cloudflight equips the employees with a PC or laptop at the workplace or for mobile use and, if required, possibly with further mobile end devices (e.g. cell phone, smartphone, tablet, token). All IT assets provided by Cloudflight to the employees on a temporary basis are the property of Cloudflight.

The IT assets are to be handled with care by the employees in accordance with their usage. Instructions for use from Cloudflight and/or the manufacturer must be considered. Provided IT assets are at least to be handled with the same care as if they were privat assets.

The IT hardware as well as the corresponding accessories (e.g. monitor) are installed exclusively by employees of the Support Function "**Internal IT**" of Cloudflight or by specialists commissioned by Cloudflight, unless there are other instructions from Cloudflight.

The telephones / cell phones / smartphones provided by Cloudflight are available to the employees as working tools within the scope of the task fulfillment and serve in particular to improve the internal and external communication, to achieve a higher efficiency and to accelerate the information procurement and the work processes. Private use is permitted to the extent that this does not affect the private use of business accounts and does not cause Cloudflight to incur additional costs. Whether and to what extent the use causes costs must be determined by the employee and clarified before use (e.g. when using the Internet flat rate or mobile phone abroad). This does not grand a general right to such a device.

The mobile IT assets are generally only intended for business trips and agreed home offices. Taking them on vacation and/or travel (including business trips) outside the European Union must be reported in advance to the Support Function "Internal IT" and requires their consent.

3.3 Software

The software used on the IT assets and in the corporate network is protected in each case by licensing regulations. The individual program packages are subject to the manufacturer's regulations. Unauthorized copies of software may not be created or passed on by the employee.

In case of uncertainty regarding the authorized use of software, the support function "Internal IT" must be consulted. Only software for which Cloudflight has acquired appropriate licenses or which has been provided to Cloudflight for use or whose license model conforms to the intended business use may be used.

Software installed on company devices by the internal IT may not be changed by the user. This does not apply to user settings (e.g. setting the font size, brightness, etc.) within applications, provided this does not impair the functionality of the IT work devices. When in doubt, seek guidance by the Support Function "Internal IT".

In the case of so-called open source software, i.e. in particular software licensed under license conditions recognized by the Open Source Initiative as "Open Source License", the use may not result in any disadvantageous consequences or obligations for Cloudflight in terms of the use or commercial utilization of the software or the overall result created with it within the scope of current or planned business operations (in particular no so-called "copyleft effect") due to the license conditions applicable to it. In case of doubt, the support function "Internal IT" and the supervisor must be informed before use.

Employees are expressly prohibited from installing software on IT workstations unless there is an operational reason for doing so. Employees are prohibited from copying company software for private use or installing it on private devices.

4. Other provisions

4.1 Workplace

The workplace must be designed by the employees in such a way that visitors or other third parties cannot gain access to personal data and/or business secrets without being authorized to do so. When leaving the workplace, the respective employee must “log off” or “lock” the IT system so that authentication (user name/password) is required before using the IT system and/or application(s) again.

In areas with public traffic, the IT systems - especially the screens - must be aligned in such a way that the risk of visitors or third parties gaining knowledge is eliminated as far as reasonably possible. This is particularly relevant when traveling, e.g., on crowded trains or airplanes. If necessary, protective films should be requested to prevent insight.

Information in paper form must be stored in such a way that visitors or other third parties cannot gain knowledge of the data. Confidential information in physical form must generally be digitized and then destroyed afterwards in accordance with data protection requirements, unless it is original or indispensable documents in paper form, in which case they must always be kept under lock and key (“clean desk”).

4.2 Use of passwords and login data

As far as technically possible, all IT systems and applications can only be used after the user has been sufficiently authenticated. Authentication is usually performed by means of two-factor authentication, exceptionally the use of the user name/password combination.

The following applies in regards to passwords:

- Each employee is required to change his initial password immediately, given this is possible.

- Passwords must be chosen in such a way that they cannot be easily guessed by third parties. For example, first and last names or birthdays as well as names of relatives are not suitable for password selection. The same applies to trivially arranged number combinations (e.g. 12345). For assistance, the instructions of the Federal Office for Information Security or the “IT Security Manual for Employees” at it-safe.at should be taken into account.

- Passwords must be kept secret. When provided on a per user basis, they may exclusively be known to the user personally (they may therefore not be passed on to colleagues or outsiders; the only exception is the passing on of initial passwords in

the course of setting up a PC, laptop or other mobile IT work devices).

- Passwords may only be entered unobserved. A password Manager must be used for storing password permanently. A password must be changed if (and only if) it has become known or suspected to unauthorized persons.

4.3 Remote access, mobile working

For accesses to the network from outside, the Support Function "**Internal IT**" provides appropriate connection options that comply with Cloudflight's security standards.

Remote access to the company network is generally only permitted via sufficiently secure security and encryption procedures (such as the Virtual Private Network (VPN), among others).

Employees are required to comply with all relevant guidelines or instructions for handling personal data even when working in mobile mode, provided that these regulations do not relate exclusively to site-related work in the company.

As a matter of principle, data must not be stored exclusively on local hard drives or data storages of end devices. Also for mobile working, data shall be stored on appropriate storages provided for the specific purposes (Git, Sharepoint, etc.) Data must not be stored on storage devices which are not owned and controlled by Cloudflight. The mobile end devices of Cloudflight are only to be permitted for mobile use if they are encrypted (even if local storage is generally to be avoided, this will be required at least temporarily in cases of poor or impossible Internet connection).

Keeping passwords secret and ensuring that there is no unauthorized access to IT assets or access to IT systems as defined in this policy also applies in particular to persons living in the same household.

Only if absolutely necessary, printouts should be made outside the Cloudflight offices, not for minor reasons such as better legibility or similar. When printed out, the hardcopies must be destroyed in a data protection compliant manner (tearing or simple data destruction with e.g. mere strip cutting is not sufficient) and must not be made accessible to third parties. If no suitable destruction is possible, the documents should be stored securely and disposed in accordance with data protection regulations after returning to the Cloudflight location.

4.4 Data exchange external data carriers

The use of external data carriers for the transport of company data is only permitted in justified and documented exceptional cases on data carriers agreed with the "**Internal IT**" support function.

When transporting company-owned data on permitted data carriers (e.g. USB drive, external hard drive, DVD, etc.), special care must be taken. The data must be protected against loss, theft and access by third parties and must be encrypted. Appropriate procedures are to be installed on the data carriers.

Only cloud services authorized by the "**Internal IT**" support function may be used in order to comply with data protection and IT security requirements. The use of private accounts for the exchange of company data is not permitted.

4.5 Protection against malicious content

Virus protection programs are used at Cloudflight to protect against malicious content. Incoming e-mail communication in particular is checked by the virus protection programs used. This may also result in the deletion of Emails and file attachments. In case an employee receives an Email with an unknown or suspicious file attachment, he is obliged to contact the support function "**Internal IT**" immediately. The unknown or suspicious file attachment may only be opened after it has been released by the "**Internal IT**" support function.

To protect against unsolicited advertising by Email, Cloudflight uses so-called spam filters. The spam filter is used for operational reasons. Due to the spam filter, e-mails may be suppressed or deleted in individual cases. Employees should ensure that, for example, when they wish to receive Email newsletters, the corresponding sender addresses are stored in their e-mail address book in order to avoid incorrect classifications.

When using communication technologies, care must be taken to avoid malicious software and recognize fraud attempts (e.g., Trojans, viruses, worms, phishing, social engineering).

4.6 Consequences of violations

If the employee notices that the protection or security of data could be endangered in any way, he must immediately contact the "**Internal IT**" support function and his supervisor. This applies in particular if the threat relates to personal data.

In case of misuse or violation of the employee's policy, Cloudflight is entitled to apply all measures permitted by labor law, including termination with or without notice. Likewise, criminal sanctions and civil consequences such as compensation for damages may be considered.

4.7 Hierarchy of standards

Insofar as provisions of this agreement conflict with other agreements or directives, this agreement shall take precedence.

4.8 Actualization and verifiability

In the course of further development of the guideline as well as technological or organizational changes, this guideline shall be reviewed regularly to determine whether there is a need for adaptions or amendments.

Changes to this guideline are effective formlessly. The employees and executives are to be informed immediately and in an appropriate manner of the changed guidelines.

Appendix

Logging and analysis procedures

(1) Insofar as necessary for reasons of data and system security or for error detection and correction, exceptionally the contents of the use of email services and internet access may be logged, or likewise exceptionally messages in email accounts may be accessed. The information obtained may only be used for the purposes specified in the first sentence and for the prosecution of criminal offenses and must be deleted immediately as soon as it is no longer required.

(2) The logs are used exclusively for the purposes of guaranteeing/restoring system security, analyzing and correcting technical errors and malfunctions, capacity planning and load distribution as well as optimization of the IT infrastructure, statistical determination of the scope of use, abuse control and prosecution as well as in the event of a suspected criminal offense. The use of the logs must comply with the principles of data protection-compliant control, in particular the principle of proportionality. If possible, the evaluation is therefore initially anonymized. If there are indications of an infection with malware, the logs must be analyzed immediately in a comprehensive, personalized manner to determine which device is suspected of being infected, and the "Internal IT" support function must take countermeasures immediately. The logs may not be used to monitor individual behavior and performance unless the conditions set out in paragraphs (5) and (6) apply.

(3) The logs are regularly evaluated after anonymization by a person commissioned by Cloudflight on a random basis with regard to the communication partners (e.g. senders of incoming and recipients of outgoing emails) as well as the addresses called up (e.g. URLs of websites). If possible, the statistical evaluation is carried out automatically.

(4) If the evaluation of the logs according to paragraph (3) does not provide any indication of a violation of the rules of this agreement ("misuse"), the logs shall be deleted. If, on the other hand, there is an indication of misuse, the employees shall be informed of this in general, non-personalized form. The employees will also be informed that in the event of continued misuse, personal evaluations of the logs will be carried out and (labor) legal consequences may arise within the framework of labor law provisions.

(5) If an evaluation of the anonymized logs - which does not have to be limited to random samples - subsequently reveals continued misuse, anonymization will not take place. If the evaluation of the anonymized logs in accordance with paragraph (3) reveals misuse, a personal evaluation of the logs is permissible with regard to the specific cases of misuse identified; if no misuse was identified, the logs must be deleted.

(6) If facts to be documented give rise to the suspicion that email or internet access has been misused to commit criminal acts, the logs and the messages themselves may be evaluated to the extent necessary and in compliance with the principle of proportionality. The evaluation may only take place in the presence of the data

protection officer, or a person authorized by the data protection officer, unless an immediate evaluation is necessary for special reasons to be communicated to the data protection officer and the data protection officer is unable to participate. Insofar as this does not jeopardize or significantly delay investigations, the employee concerned must be notified of the evaluation and allowed to participate.

(7) The result of the personal evaluation in accordance with paragraphs (5) and (6) shall be documented. The employee concerned shall be informed about the personal evaluation and its essential results as soon as this does not jeopardize the sense and purpose of the personal evaluation; upon request, the employee shall be informed about the complete evaluation concerning him. Deferring the provision of information to the employee for more than three months requires the written consent of the data protection officer. The employee concerned has the right to comment on any personal evaluation concerning him. If the suspicion of misuse is invalidated, all personal data resulting from the monitoring procedure shall be deleted unless the employee objects.

(8) Anonymization must be reestablished after maximum three months after the date of the last identified misuse.

(9) It is not permissible to evaluate the logs in order to obtain information about the use of email and internet access in connection with functions that require special protection (employee representatives, etc.).

(10) The logs must be kept in a specially secured place to prevent unauthorized access.

1.2.2022, Version 1.1

cloudflight