PLANIT//LEGAL

Name	Version	Date	Editor	Modification
Privacy Policy	0.9	2023	DPO	Preparation
Privacy Policy	1.0	2024	DPO/Elina Sinisalo, Marc Hentz	Coordination
Privacy Policy	1.1	May 2024	DPO/Elina Sinisalo, Marc Hentz	Finalizing Version for announcement

Privacy Policy

Dewpoint Therapeutics GmbH

Status May 2024

Content

1. Aim of this Privacy Policy

Dewpoint Therapeutics GmbH (hereinafter: Dewpoint or Company) is responsible for data protection and must ensure adequate protection of personal data under its control. In addition, Dewpoint must ensure adequate protection of the privacy rights of data subjects. To this end, Dewpoint has defined responsibilities, established data protection management processes, and taken technical and organizational measures that are described in this policy and are binding for all Dewpoint employees.

This policy includes a commitment to strive for privacy-compliant design of all Dewpoint business processes.

2. Scope of Application

This Policy applies to employees, interns, Dewpoint contractors, and other employees of Dewpoint (hereinafter: **Employees**). It is legally binding and applies both on and off Dewpoint's business premises and must be observed by Employees when carrying out their duties for Dewpoint.

3. Definitions

For the purposes of this Policy, the following terms shall have the meaning described here. In addition, the definitions of the General Data Protection Regulation (hereinafter: **GDPR**) and the German Data Protection Act (hereinafter: **BDSG**) apply.

Processor means the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

BDSG means Bundesdatenschutzgesetz (German Federal Data Protection Act) from 30 June 2017 (BGBl. I S. 2097) and as amended from time to time.

Personal Data Breach means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

GDPR is the Regulation (EU) 2016/679 of the European Parliament and the European Council of the 27 April 2016 to the protection of natural persons with regard to the processing of Personal Data and rules relating to the free movement of Personal Data and repealing the

Directive 95/46/EG (General Data Protection Regulation) as amended.

Personal Data means any information relating to an identified or identifiable natural person (data subject), such as a name, e-mail address, photographs, video or audio recordings. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It is not important that the name be mentioned. It is sufficient that it is possible to find out who the person is. Therefore, even information that at first glance does not appear to be associated with a natural person may be personal data, such as IP addresses.

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data (Art. 4 No. 7 GDPR). The Controller for the purposes of this Policy is Dewpoint.

Confidential Information Confidential information is all information from and about Dewpoint, as well as all information acquired in the course of working for Dewpoint, if and as long as it has not been made public in a lawful manner (e.g. information in company press releases). This includes in particular information that could cause damage to Dewpoint, its customers or Employees if discovered by unauthorized persons (e.g. development data, strategy plans, contract documents, etc.).

4. Responsibilities

This section defines the roles and responsibilities of management, the Data Protection Officer, Employees and the IT department.

4.1. Management

The management is responsible for the organization's compliance with data protection law.

Specifically, management

- issues rules and regulations related to this Policy and Dewpoint's privacy organization,
- delegates duties and responsibilities under this Policy,
- has the right to make final decisions on all core data protection matters, including, but not limited to, implementing policies, reporting incidents, or responding to regulatory proceedings,
- may at any time assume responsibilities under this Policy and the Dewpoint Privacy Organization as described herein or in another context,
- is responsible for appointing the DPO and ensuring that the DPO has the information, skills and resources necessary to perform his/her duties.

4.2. Data Protection Officer

Dewpoint has appointed a Data Protection Officer according to Art. 37 GDPR and Section 38 BDSG. The Data Protection Officer is independent and in particular not bound to Management instructions in performing the tasks and duties. You can reach the Data Protection Officer by e-mail: dataprotection@dewpointx.com.

The Data Protection Officer shall

- inform and advise management and Employees on all matters relating to the protection of personal data, including their duties in this regard; he/she is obliged to maintain confidentiality with regard to the data subjects,
- monitor compliance with the Privacy Policy and with the GDPR,
- report to management and have the right to be heard in matters relating to the protection of personal data,
- train Employees in the protection of personal data,
- advise, upon request, in the context of data protection impact assessments and the monitoring of their implementation; and
- cooperate with data protection authorities, in particular as their point of contact on matters

relating to the processing of personal data, including prior consultation pursuant to Article 36 of the GDPR and providing advice on other issues as appropriate.

The DPO shall have the right to obtain information and have access to business premises, data processing equipment, and documents concerning Dewpoint's business processes and procedures for processing personal data. He/she shall be involved in the planning of new IT systems, the modification of existing IT systems and other measures that may have an impact on the protection of personal data.

4.3. Employees

All managers in the Company whose departments process personal data, as well as all Employees in the respective functions who regularly handle personal data, are responsible for implementing operational self-monitoring (see Section 5). Each Employee is responsible for adhering to this Policy and the requirements of data protection law in his or her area of responsibility.

Before a new IT system is put into operation, the employee responsible for the IT system in the respective function is responsible for ensuring that it is operated in accordance with internal company and legal requirements and that these requirements are met during operation. The individual will be supported by the IT function.

4.4. IT Function

Dewpoint Therapeutics Inc. is providing the services of an IT function for Dewpoint. The IT function is responsible for the overall administration of the IT systems. In addition, the IT function implements the requirements of the employees who are technically responsible for an IT system and administers the IT systems.

5. Data Protection Organization and Data Protection Management

Dewpoint is committed to complying with data protection laws and follows the principle of operational self-control. As a result, it is part of Dewpoint's corporate culture to ensure that data protection laws and other legal requirements regarding data protection are implemented in a manner that is reasonable, economically justifiable, and technically and organizationally feasible. This policy describes the essential components of Dewpoint's data protection organization. This policy will be reviewed periodically and may be updated from time to time.

5.1. Obligation to Maintain Personal Data in a confidential manner

Employees are required to maintain personal data confidentiality. A document to this effect must be signed when the employment contract is concluded. The Employee receives a copy of the document and information about his or her confidentiality obligations.

5.2. Transfer of Personal Data

Employees may only disclose Personal Data to other Employees or third parties if there is a legal justification for doing so. Personal Data may only be transferred to third countries outside the European Union if adequate data protection safeguards are in place or, in an exceptional case defined by law, an authorization exists. In case of doubt, the Data Protection Officer should be consulted.

5.3. Notification of new procedures and Records of Processing Activities

Employees with technical responsibility for an IT system shall inform the DPO about the IT systems used to process Personal Data and shall notify the DPO of the introduction of new IT systems and significant changes to existing IT systems.

When establishing procedures for the processing of Personal Data, the employee responsible for the IT system shall ensure that technical means are chosen that ensure an adequate level of protection of Personal Data and shall use only such means as are appropriate to comply with data protection requirements. The employee responsible for the IT system shall implement and document technical and organizational measures to adequately protect Personal Data.

The Records of Processing Activities shall map all operational processes where personal data, e.g. of Employees, customers, suppliers or other natural persons, is processed. The employees responsible for an IT system provide the information required by Article 30 of the GDPR in the document template provided for this purpose. The DPO stores these documents in his documentation system (Records of Processing Activities) and assists the employees responsible for the IT system in preparing them.

The DPO shall make the records of processing activities, or parts thereof, available to third parties if required to do so by law or by management. The records of processing activities shall reflect all operational processes to the extent that personal data are processed.

5.4. Privacy by Design and by Default

When implementing procedures for processing Personal Data, the employee responsible for the IT system shall ensure that IT systems are selected that enable data protection-compliant operation (privacy by design) and that they are configured in such a way that data protection-compliant operation takes place (privacy by default). In particular, retention and deletion periods are defined in accordance with data protection requirements and access rights are configured accordingly. The IT department and the Data Protection Officer support the employees responsible for the IT system in this process.

5.5. Data Protection Impact Assessment

Before implementing procedures for the processing of Personal Data, the person technically responsible for the IT system shall assess the risks involved for the rights and freedoms of the data subjects concerned. If he/she considers the risk to be high, he/she shall consult the DPO and carry out a data protection impact assessment. The DPO may identify a high risk independently of the person technically responsible for the assessment of the IT system and report it to the person responsible, who will then initiate the DPIA process.

In order to carry out the DPIA, the processing operations, the necessity and appropriateness of the processing operations, the risks to the rights and freedoms of data subjects and the measures to mitigate those risks shall be documented. The DPIA will be conducted in consultation with the DPO. If there are no adequate measures available to address the identified risks, Dewpoint will not carry out the processing. If a significant risk remains during the implementation of the procedure, management will decide on the implementation of the processing procedure.

5.6. Assignment and Assessment of Processors

Before assigning data processing to a processor, the employee responsible for the IT system assesses whether the processor provides adequate guarantees and has taken appropriate technical and organizational measures to ensure that the processing of personal data is carried out in accordance with the requirements of internal company specifications and the requirements of data protection law. During the course of the contract, the responsible Employee regularly checks whether the technical and organizational measures have been implemented and are adequate for the requirements of the contract. The content, scope and

frequency of the reviews will depend on the nature, scope, circumstances and purpose of the processing. In any case, the responsible Employee must request and assess the processor's concept for technical and organizational data protection.

He/she shall ensure that the assignment of the processor is made by means of a data processing agreement that complies with the requirements pursuant to Art. 28 GDPR.

The responsible Employee may seek advice from the Data Protection Officer. In any event, the Data Protection Officer shall be consulted prior to the assignment of processors outside the European Union.

5.7. Joint Responsibility

When implementing an IT system, the employee responsible for the IT system shall assess whether and, if so, which third parties have joint influence with the controller on the processing of Personal Data. If the controllers jointly determine the purpose of the processing, he/she shall ensure that a joint responsibility agreement is concluded between the controllers involved and that the data subjects are informed of its essential contents.

The responsible Employee may seek advice from the Privacy Officer.

5.8. Incident Reporting

A personal data breach is an incident in which personal data is unlawfully disclosed to a third party or deleted. Therefore, not every violation of the GDPR automatically constitutes a data breach; rather, personal data must be unlawfully disclosed or deleted as a result of the violation. If an Employee becomes aware of an actual or potential Data Protection Incident, he or she must immediately report it to the Data Protection Officer, his or her supervisor, or senior management. To report the Data Protection Incident, the Employee must provide his or her name and contact information (e-mail, telephone number, etc.) for any inquiries and describe the Data Protection Incident as accurately as possible (time and place, data and systems involved, actions taken, etc.). The Employee may not report any Data Protection Incident to any other person, institution or authority, whether inside or outside the Company.

In the event of a privacy incident, the recipient of the report will inform management, the Data Protection Officer and the IT department. The IT department will immediately initiate measures to secure the affected IT systems and protect the affected personal data.

The DPO, management and, if applicable, the IT department shall directly coordinate what additional measures should be taken to secure the affected IT systems and protect the affected Personal Data, and to determine whether a notification should be submitted to the relevant data protection authority. Management will make the decision whether or not to report the data incident. The DPO may make the notification at Dewpoint's direction.

5.9. Information requirements

When collecting data, various information must be provided to the data subjects. Information must be provided about (Art. 13 GDPR):

- the name and contact details of the controller;
- the contact details of the Data Protection Officer;
- the purposes for which the data are to be processed;
- the legal basis for the processing and, if the processing is based on legitimate interests, also an indication of those interests;
- the recipients or categories of recipients;
- where applicable, the intention to transfer the personal data to a third country or to an international organization and appropriate safeguards for the protection of the data in this case;
- the duration of the storage or criteria for determining this duration;
- the data subject rights and the right to lodge a complaint with a supervisory authority;
- whether there is an obligation to provide the personal data, and what the possible consequences of not providing it would be; and
- the existence of automated decision-making pursuant to Article 22(1) of the GDPR and the logic used for this purpose.

The information must be provided in a precise, transparent, understandable, and easily accessible form, in clear and simple language (Art. 12(1) GDPR). The information can be provided in electronic form, e.g. on a website. Dewpoint will provide the necessary information to the data subjects. Dewpoint has a privacy policy on its website, which also informs applicants about the processing of their data as part of the application process. Employees receive an Employee Privacy Notice as an attachment to their employment contract. Before introducing new IT processes, Dewpoint, with the assistance of the Data Protection Officer, checks whether

information requirements need to be met.

5.10. Data Subject Requests

All Employees are required to direct requests regarding the rights of data subjects (e.g., requests for information, correction, deletion, blocking or transfer of personal data) to the Privacy Officer. Dewpoint, in consultation with the Data Protection Officer, will promptly contact the data subject and politely request that the request be clarified if the request or its scope is unclear. The data subject must prove his or her identity if there is reasonable doubt about the identity of the data subject, e.g. by providing a photocopy of an official identification document such as a passport, driver's license or national identity card, or by requesting additional information such as date of birth, address or similar information and comparing it with the data held by Dewpoint for identification purposes. The rights of the data subject are personal rights, and Dewpoint is required to disclose or amend a person's personal information only if it can prove that the instructions came from that person.

If the DPO believes that the data subject's request is unjustified, he or she shall inform the data subject accordingly. Otherwise, he or she shall forward the request to the employee with functional responsibility. The employee with functional responsibility shall inform the Data Protection Officer within 14 days whether personal data are processed by the person making the request. The Data Protection Officer and, if necessary, the IT department will assist in processing the data subject's request.

If the data processing is based on consent, the data subject has the right to revoke this consent at any time with effect for the future (Art. 7 (3) DSGO). The data processing carried out up to that point remains lawful but must be discontinued for the future. If there is no other legal basis for storing the data, the data stored on the basis of the consent must then be deleted.

The data subject has the right to object to the processing of the data, provided that the processing is carried out to protect the legitimate interests of the controller or of a third party. In doing so, the data subject must provide reasons arising from his or her particular situation. In this case, the controller may only continue to process the personal data if

- it demonstrates compelling legitimate grounds for the processing which override the interests of the data subject, or

- the processing serves the assertion, exercise or defence of legal claims.

An unconditional right to object, the assertion of which shall in any case stop the processing, applies in the event that personal data are processed for direct marketing purposes (including profiling for direct marketing purposes).

The People & Culture Department is responsible for receiving revocations or objections from Employees. Upon receipt of a revocation or objection, People & Culture will notify the DPO. In the case of a revocation, the DPO will consider whether there is another legal basis or, in the case of an objection, whether there are compelling reasons in favor of the data controller. The DPO will consult with People & Culture on how to proceed. If the data subject has requested notification of the implementation of the revocation of consent or the objection, People & Culture or the Data Protection Officer shall notify the data subject.

Requests from data subjects regarding their rights (e.g., access, rectification, erasure, restriction, data portability) will be forwarded to the Data Protection Officer. The Data Protection Officer will evaluate the request, propose action to management, and notify the data subject of the action taken and/or provide information as requested and required by data protection law or this Policy.

5.11. Accountability, Data Protection Documentation and Audits

To ensure adequate documentation of compliance (accountability) as required by law, Dewpoint will maintain conclusive and traceable written documentation of the measures taken. The employees responsible for the IT system and the Data Protection Officer keep this documentation for the area of data protection organization. Independently, the Data Protection Officer monitors compliance with privacy laws when introducing new IT systems and conducts general privacy audits.

6. Technical and Organisational Data Protection Organisation

To ensure compliance with privacy laws in Dewpoint's business operations, the following rules and regulations apply to all Dewpoint Employees. Dewpoint will periodically review and may update this policy from time to time.

6.1. Personal Conduct at the Workplace

As part of the onboarding process, People & Culture will issue a key to access the Company's premises and, if applicable, office buildings and other buildings on the Company's premises. People & Culture, Lab & Facilities Operations, or IT will document the issuance of keys. Employees must treat the issued key(s) with confidentiality and report any loss to People & Culture immediately.

Unless Employees have their own office that is locked when they are away, access to the PC must be prevented when leaving the workstation. This can be done by logging off the system, locking the workstation, or activating a password-protected screen saver. In any case, Employees must ensure that no one can access system resources under the user ID of an absent Employee.

Employees must shut down workstation computers before turning them off. The IT department must be notified if IT processes are significantly slowed or if error messages and system crashes occur frequently.

Business-critical data must be stored on network drives (for regular backups) and not on local hard drives (e.g., C drives) on workstations. If Employees are not connected to the corporate network while processing business data, new files must be immediately transferred to "secure" network drives the next time they connect to the corporate network.

All data that is no longer required for the Company's business activities and that is not subject to a contractual or legal retention obligation will be deleted.

If Employees do not have their own office, which is locked at all times during their absence, they must always leave the workplace in a clean condition ("clean desk"). When leaving the workplace, Employees must ensure that confidential information (whether on paper or electronic media) is not accessible to unauthorized persons and is not at risk of loss. Unauthorized persons must be prevented from accessing media (such as CDs, DVDs, USB sticks or external hard drives) or paper-based documents at the workstation.

Employees must remove documents when leaving meeting rooms. This is especially true for written documents on flipcharts/copy boards.

Screens and printers in Dewpoint offices must be set up to prevent unauthorized viewing and access by outside parties. A password-protected screen saver must be activated on all PCs, which will automatically activate no later than 15 minutes after the last keystroke or mouse action.

6.2. Public Authorities' and other Third Parties' Requests for Information

In the event of a request for information from a public authority (police, public prosecutor, etc.) or other third party, the Employee receiving the request will handle the request in accordance with the internal policy applicable to the specific case. If he or she is not aware of any internal guidance, he or she will refer the request to management or the Data Protection Officer for handling or advice on the procedure.

6.3. Private Use of Business Hardware and Communication Systems

The personal use of hardware (computers, servers, tablets) and communication systems is generally prohibited. In particular, Employees may not use the email system or telephones for personal communications. This does not apply to limited personal telephone calls, provided that the quality and quantity of work performance is not adversely affected.

Dewpoint reserves the right to check compliance with this rule on a random basis, if necessary through automated technical means.

Personal use is defined as any activity that is not related to the business activities of Dewpoint or its business partners and that does not harm the interests of Dewpoint or the relationship between the user and Dewpoint. Business use includes any user activity that is directly or indirectly related to Dewpoint and its business or the relationship between Dewpoint and its Employees.

6.4. Email and Calendar

Dewpoint electronically archives incoming and outgoing email in accordance with legal requirements. Authorized individuals can access individual emails in accordance with legal requirements.

Employees using the e-mail system may not include personal correspondence in business e-mails. They must immediately delete any personal e-mail they receive. If an incoming business

email contains private information, it must be treated as business content. If it is not detrimental to Dewpoint's overall workflow, the sender of the email should be asked not to include any more personal correspondence in company emails and to use the email address for business purposes only.

Dewpoint may monitor the use of email accounts for compliance with this policy. This will be done on a random basis and in the event of anomalies (e.g. suspected misuse). If email is forwarded to others, it may only be done in the form of a copy and with due regard to the need and legal justification to provide the recipients with the information contained in such communications.

Employees must not open emails or email attachments that are suspicious in terms of sender, subject, content or salutation. If in doubt, Employees must contact IT (submit a ticket or report as possible phishing) before opening an email or email attachment and, if necessary, contact the sender (only if known to the receiver) to determine whether the message is trustworthy and intentionally sent. Refer to Dewpoint’s guidelines on cybersecurity for more information.

Before sending an email, Employees must ensure that the recipient addresses are correct. The same applies when using the reply function. Additional email addresses should only be included if necessary in the individual case.

When sending email to a large group of external recipients, the email addresses must always be placed in "bcc" to prevent recipients from seeing the email addresses of other recipients. An "open" entry of the email address in "cc" is only allowed if it can be assumed that the recipients concerned agree to the disclosure of their email address to other recipients.

Employees use the calendar feature in Outlook. They can also view other Employees' calendars to coordinate appointments. However, Dewpoint has configured the application to only show whether the Employee is available or not. Employees can voluntarily give other Employees access to their calendars and provide them with more details about individual appointments.

6.5. Internet

Subject to revocation at any time, Employees are permitted to use Internet access at their workstations for personal purposes to a limited extent, provided that the quality and quantity of their work performance and the availability of Internet access for business purposes are not

adversely affected. This permission applies only to the use of Internet access for lawful purposes (e.g., use of webmail accounts, access to legitimate, official websites).

Accessing, providing, or distributing illegal content (e.g., racist, pornographic, or other types of content) or using the Internet to infringe intellectual property or other rights by uploading or downloading copyrighted or criminal content is prohibited.

You may not upload files to external networks or computers, nor download files from the Internet. The only exception to this rule is downloading files in PDF format from reliable and secure sources. If there is any doubt about the security of the source, the Employee must refrain from downloading content and consult with the IT department.

6.6. Remote Access, Home and Mobile Office

Where remote access to Dewpoint IT systems is required, Employees may be granted such access. The establishment of such remote access and/or permission to perform activities in the home or mobile office requires prior approval by management and the IT Department. Personal data and confidential information must be protected in the Home and Mobile Office and/or during remote access in a manner that prevents unauthorized access to the information by third parties (including persons living in the same household).

6.7. Cloud Services

Employees may not use cloud services such as Dropbox, Google Drive, etc. for business purposes unless permission has been granted by the IT department.. They may only use communication and storage media or services provided by IT for the exchange of official information. Instructions from the IT Department must be followed. If the communication and storage media or services provided do not meet the business requirements, the IT department must be informed, and the situation must be handled in accordance with its instructions.

6.8. Access to Directories and Network Folders

To the extent that Employees grant other users access to directories or folders, they must ensure that this is done only to the extent necessary and within the scope of the other users' responsibilities. For example, third party access to e-mail may violate the privacy rights of third parties if unauthorized third parties view their e-mail. In particular, separate folders and directories containing non-public confidential information must not be made available for

unrestricted access throughout the corporate network.

6.9. Phone

Employees may make confidential telephone calls only in private and in a manner that prevents unauthorized persons from overhearing confidential communications. Only the Employee or the Employee's designee may provide access to the Employee's personal mailbox.

6.10. Transport Encryption

Every Employee is required to use encrypted communication channels whenever possible. This is especially important when using web applications. Unencrypted communication may allow access to login credentials and other data that may be vulnerable to misuse. If necessary, Employees must stop processing and transmitting data if it can only be done through unencrypted communication channels. In this case, Employees must consult with IT.

Unencrypted email outside the corporate network is like a postcard: anyone involved in the communication process can read and copy the contents of such email. Therefore, Employees should not send unencrypted e-mail with confidential content outside the corporate network. This is especially true for confidential e-mail. If it is not possible to encrypt the e-mail, information in attachments must be protected from unauthorized access by encryption or password protection.

6.11. Mail

Mail that contains an Employee's name in the address field before the company name, or that contains the words "personal," "confidential," "private," "secret," or the like, must be delivered personally and unopened to the designated Employee. Other mail may only be opened by a person designated by management. The mail will then be forwarded to the appropriate person or team.

When mail is sent, the person authorized to receive it at the recipient's end must be identified whenever possible. If confidential information is involved, the address field must contain the words "personal" or "confidential". If it is possible to infer certain facts about the communication from the sender's information, the exact sender must not be identifiable from the outside. In the case of window envelopes, the window size and paper size must be selected in such a way that no further personal data or confidential information is revealed by the

movement of the paper. Only opaque envelopes may be used for mailing.

6.12. Fax

There is an increased risk of misdirection or unauthorized access when communicating via fax. Therefore, Employees should avoid using fax machines to transmit personal data and confidential information whenever possible.

If personal data or confidential information must be transmitted by facsimile, the recipient must be notified of the transmission prior to sending the facsimile in order to verify receipt. Before sending a fax, the Employee must ensure that the recipient's number is correct. In addition, before starting the transmission process, it is necessary to double-check that the destination number matches the number shown on the display. If it does not match, the user must cancel the transmission.

Employees should not leave faxes containing personal data or other confidential information unattended in the fax machine and should remove them immediately after printing.

6.13. Scanners, Printers and Copy Machines

If scanned documents are stored directly in a network directory, Employees must ensure that the network directory is protected from unauthorized access. Only public documents may be scanned directly into network directories that are accessible to the entire organization.

Prints containing Personal Data or other Confidential Information must not be left in the printer unattended and must be removed from the printer immediately after printing. The same applies to copiers.

6.14. Laptops und Smartphones

Employees should never leave laptops unsecured at any time. They must ensure that they are under constant supervision if they are stored outside restricted areas. If a laptop is lost, stolen or destroyed, the IT department and, if necessary, the police must be informed immediately.

When using a laptop in a public area, Employees must ensure that others cannot view the content displayed on the laptop screen. If such protection cannot be provided, the laptop should not be used in public.

If Confidential Information is stored on the hard drive of a laptop, the Employee must ensure

that the hard drive cannot be read without authorization. The IT department should be consulted on this matter. The use of a BIOS password or encryption of the hard drive is strongly recommended in consultation with IT.

To ensure that the system is up to date, Employees must ensure that scheduled updates (especially virus scanner and operating system) are installed on the device. This is done automatically on a regular basis when you log on to the corporate network.

The above rules also apply to mobile devices such as smartphones. However, it should be noted that these devices often have limited data security measures. Therefore, Employees must immediately delete data from such devices when it is no longer needed. In particular, unauthorized reading of memory cards must be prevented.

6.15. USB-Sticks and other Mobile Storage Media

Employees may use USB sticks, optical storage devices, external hard drives, memory cards and other portable storage devices only for business purposes. It is prohibited to store Company data on personal USB flash drives, optical storage devices, memory cards, external hard drives and other portable storage devices. In fact, Employees may not plug such storage devices into or connect them to company computers at any time.

Employees may only run software from a USB flash drive or other external storage device that has been approved by the IT Department. If confidential information is stored on a company USB flash drive or other external storage device, the drive or the data stored on it must be encrypted before being taken off Dewpoint premises.

Employees may not connect business USB thumb drives or other external storage devices containing Confidential Information or personal data to computers outside the Company. When connecting to non-business computers, use a non-recordable media, such as a CD/DVD or write-protected USB flash drive, that does not contain any Confidential Information other than the information needed for the specific purpose. Employees may not connect external media or USB sticks to their own computers without prior review and approval by the IT Department.

6.16. Password Protection

The IT department and/or the IT security officer shall publish guidelines for IT security,

including password protection, based on current technical possibilities for preventing misuse. These guidelines are binding and are reviewed and enforced in an appropriate technical and organizational manner.

If Dewpoint does not have the password parameters predefined by the system, it is important to ensure that the password is not easily guessed. A password should be at least 8 characters long and should always be a combination of upper- and lower-case letters, numbers and special characters. Problematic are trivial passwords such as "ABC" or keyboard sequences (e.g. "qwert" or "asdfgh"), all kinds of names (e.g. of friends, acquaintances, colleagues, family members, pets), cities and buildings, designations, cartoon characters, car brands, license plates, terms, dates of birth, phone numbers, common abbreviations, etc.

Employees must keep passwords strictly confidential. The obligation to keep passwords confidential also applies to co-workers and supervisors. However, if a password has been disclosed in violation of this Policy, for example, to allow a third-party access to an account in an emergency, the password must be changed immediately. It is prohibited to store passwords in paper form at the workstation or in unencrypted electronic form on a computer or external data carrier.

6.17. Misuse of IT

The IT Department may suspend and audit accounts upon suspicion of misuse of IT systems or hardware. IT may not conduct automated monitoring and evaluation on a regular basis but may do so upon suspicion. If monitoring is generalized to prevent misuse, Employees will be informed of the intended action. The IT department may only disclose information that is necessary to investigate misuse.

6.18. Maintenance Works

The IT department may view user profiles or sensitive data during maintenance or IT-related reorganizations. This information is not used for any other purpose, except in cases of suspected misuse of hardware or IT systems or criminal activity.

6.19. Loss of Hardware

If hardware is lost, IT must be notified immediately. IT will take steps to mitigate the risk associated with the loss. These measures may include, but are not limited to, localization,

remote wiping, blocking of accounts (email system, VPN, etc.) and monitoring of accounts. If personal data is collected in this context, it will only be used to locate devices or to detect misuse and to assist law enforcement authorities, if necessary.

6.20. Bring your Own Device

The use of personal hardware or hardware not purchased by Dewpoint for business purposes is prohibited and only permitted in exceptional cases with the approval of IT. Connection of such hardware to Dewpoint hardware or IT systems is allowed only if approved by IT.

If the IT department has approved the use of personal hardware, special attention must be paid to data protection and data security. In particular, appropriate measures must be taken to prevent unauthorized access by third parties.

6.21. Recycling of Documents and Hardware

Dewpoint works almost entirely without paper. Documents, if any, containing personal data or confidential information must be disposed of in a separate collection container. For further processing, these documents must be destroyed to at least security level 2 (DIN 66399).

Documents containing personal data or confidential information may only be disposed of in the normal wastepaper basket in exceptional cases and only if they have been previously shredded to security level 2 (DIN 66399) or higher.

Electronic data carriers (e.g. CDs, DVDs, external hard drives, memory cards, USB sticks) must not be disposed of in the normal waste disposal system. Instead, they must be turned over to the IT department for destruction, which will ensure at least security level 2 destruction (DIN 66399).

6.22. Visitor Process

Dewpoint offices can only be accessed with a key fob/badge. Visitors are required to register upon arrival. Dewpoint will only grant them access to predefined areas. Visitors will not be granted access to other areas without the supervision of a Dewpoint Employee. In particular, they may not be left alone in areas where personal data and confidential information may be accessed. Visitors must be accompanied by Dewpoint personnel throughout their stay.

Dewpoint may grant permanent visitors the right to remain unaccompanied in designated

areas for a period of time. Management will approve the permit.

The Executive Leadership Team (ELT) and Managing Director of the GmbH