Terms and conditions for the private use of communication media (internet/e-mail/telephone) of the company Bosch.IO GmbH

For the private use of company communication media (internet/e-mail/telephone) provided by Bosch.IO GmbH ("Company"), the following regulations apply to employees:

1. Scope and form of private use
    a. Private use of the company internet connection as well as the telecommunications systems and business e-mail accounts is permitted, provided that the availability of IT systems is not compromised for business purposes, the private use has no negative effects on the proper performance of work duties and ultimately that the use is in accordance with the provisions of these terms and conditions of use.
    b. The company does not guarantee that the communication media will be available undisturbed to employees at all times and all websites will be accessible via the internet provided. In particular, for reasons of IT security and for preventing a loss of expertise, the company is entitled to block the access to some websites, groups of websites or certain portals.
    c. The company reserves the right to prohibit or restrict private use of company communication media in individual cases temporarily or permanently in the event of any violations of the terms and conditions of use.

2. Code of conduct
    a. When using the company communication media, the statutory provisions and these terms and conditions of use must be observed.
    b. Retrieving, offering, distributing or processing illegal content, particularly content which violates criminal regulations, data protection, personal rights, licensing or copyright provisions, as well as content which is extremist, harmful to minors, sexist, defamatory or unconstitutional, is expressly forbidden. Websites with illegal content, for example which is harmful to minors, extremist or criminal can be blocked by the company.
    c. As part of private use, it is not permitted to use company communication media for pursuing additional business purposes outside the company.
    d. Installing software for private use on company hardware requires the prior approval of the company.

e. Data and expertise of the company may not be transferred to, or stored in, cloud-based services (e.g. Dropbox) outside the company.

f. When opening attachments or links as part of the private use of business e-mail accounts, special care is required and, in cases of uncertainty, RB-CERT must be consulted, especially for e-mails from unknown senders, SPAM e-mails or e-mails with dubious content.

g. As part of the private use of communication media, no additional cost to the company may be incurred, such as by accessing fee-based websites or calling special numbers which are subject to a charge (e.g. 0900, etc.), with the exception of costs for the infrastructure or other insignificant costs.

h. It is advisable to delete private e-mails or e-mails with personal content (e.g. mail from the company doctor, social counseling) either immediately or save them separately in a folder marked as private.

i. As part of any private correspondence, employees are personally responsible for informing the recipient that the e-mail address used by the employee is a business address, and that incoming messages are filtered and controlled to protect the IT security from harmful content.

j. With the termination of the employment contract, the e-mail address and the internet services are no longer available for further use; all private content must be deleted before the employee departs.

3. Data acquisition and data analysis

When using electronic data, data acquisition and an evaluation are carried out as described below.
Electronic data is defined as data which is acquired when using internet services, including data from e-mail accounts and intranet services provided by Bosch, such as Bosch Connect (internet and intranet services will be referred to as “internet services” below) and electronic data, which is accessible to one or more employees (e.g. C/U drive, encrypted files, files on Bosch data carriers).
A distinction between business and private use of internet services is not made by any technical means. The data acquisition and evaluation described in the following points also extends to the area of private use of internet services.

a. Intended purpose

i. Protection of the IT infrastructure

ii. The protection of electronic data for the purpose of evaluating any violations to the compliance requirement or court proceedings, administrative directives or for legal defense, in so far as an obligation or legitimate interest exists for Bosch to evaluate company data is (including so-called Pre-Trial Discovery)

iii. Access to electronic data in the case of the non-availability of an employee

b. System description

i. To achieve the purposes mentioned under 3.a.i., the following measures are taken by Bosch:

- Use of automated URL blockers to the firewall/proxy systems for filtering and, if required, the suppression of illegal content and malicious software.
- Blocking individual websites, e.g. websites with illegal content, website e-mail or online storage.

Use of antivirus software for all website access. An automated scan in content data also occurs for encrypted traffic to filter out malware and automatic decryption of encrypted data and subsequent re-encryption.

- Inventory of hardware and software versions.
- Use of spam filters.
- Data acquisition in systems between the internet and the BCN or within the BCN (e.g. internet proxy servers, mail gateways, VPN access and other bridge systems): Recording of traffic data (traffic data is data that is collected and processed in the provision of internet services and includes source and destination IP addresses, user ID, date and time and URLs) and content data, if absolutely necessary (e.g. e-mail content, Word/Excel files) for a maximum time period of three months. An automatic decryption of encrypted data and a re-encryption is carried out.
- To protect the IT infrastructure and the security of the IT operation systems, the data streams are continuously recorded on a network basis (buffered if required) and promptly checked for malware, using for example antivirus software, intrusion detection and intrusion prevention systems. Individual data links can be interrupted by firewall or proxy systems if necessary to prevent the unintentional loss of intellectual property. An automated evaluation of the data or the employee is not carried out.
- A manual evaluation only occurs if there is a reasonable suspicion of a security incident or intrusion attempt into the IT infrastructure (posing imminent danger).

- Personal data is stored for the purpose of ensuring the proper operation of the electronic communication media, e.g. for error analysis and correction, system optimization, and only to be used for these purposes.

ii. In order to achieve the purposes described under 3.a.ii, a specific data acquisition relating to a person, analysis and distribution of electronic data can take place in the following cases:

- In the case of a concrete, justifiable suspicion of a violation to the compliance requirement, in particular
    - concrete suspicion of a crime or an offense
    - concrete suspicion of another significant violation to the employment contract (e.g. a violation of the antitrust law in Germany)
- In court proceedings, in administrative directives or for legal defense, in so far as an obligation or a legitimate interest exists for Bosch to evaluate company data (including so-called Pre-Trial Discovery)

When detecting, analyzing and distributing data, the relevant laws must always be observed.

If there is a danger of data being deleted and therefore that important evidence could be destroyed (posing imminent danger), in accordance with a legal assessment by the relevant central departments of Robert Bosch GmbH (C/LS, C/TX, C/IP, C/HPL, C/ISP), the data is “frozen”, i.e. the current state of the data is backed up.

Personal data, which is stored for backup purposes, may only be used for these purposes.

Initiating an evaluation must be made by the aforementioned central divisions of Robert Bosch GmbH and/or C/AU or through the HR, HRL or the BV for site-specific cases.

Before an evaluation of electronic data, a data protection audit and review must be carried out by C/ISP or the DSO organization responsible – the abovementioned central departments support this in accordance with their responsibilities.

The evaluations are documented. If a violation is discovered, the employee is confronted with the findings. Then the opportunity for a hearing is given to him or her.

Electronic data, which was collected according to paragraph 3, may be forwarded to the company bodies who are responsible, as well as responsible bodies of Robert Bosch GmbH or third parties (e.g. law firms, technical service providers, courts,

authorities) for further processing, however, only to the extent that is required, after review by the central divisions of Robert Bosch GmbH, with regard to the achievement of the purposes referred to in the specific cases in this paragraph 3, permissible by data protection law.

As far as criminally relevant content is concerned, this data may be additionally forwarded to the prosecuting authorities.

Use of the aforementioned data for further performance or behavior control is not permitted.

iii. Access is allowed to electronic data for achieving the described purpose of access below under 3.a.iii in the case of the non-availability of an employee, once an attempt has been made to contact the employee for obtaining his or her consent for access several times without success. This is provided that business operations deem it to be urgent (e.g. access to a specific document in order to continue business procedures, creating a message of absence).

The DSO, DSP and the disciplinary superiors responsible must be informed of this, and involved, at an early stage. The applicant must define the urgency of the procedure and the subject of the search, and it must be documented and demonstrated that this approach does not outweigh any legitimate interests involved.

With the authorization and approval of the access by the responsible DSO (or representative) and the disciplinary superiors, the applicant may then proceed in the presence of an accompanying person. As part of the access – if necessary – a message of absence is created.

The procedure is logged by the applicant after successful access and the account is blocked by the IV partners or local CI.

In the log, the following points are documented:

- User account affected
- Persons involved
- Date and time of the login
- List of directories, files, systems or data that have been accessed
- Time of the logout

The log is signed by the applicant and the accompanying person.

The employee affected is directly informed of the procedure by the applicant upon return. Unless the account was blocked for the access, the affected person must initiate the activation of his or her account and change the password.

c. Duration of storage

Personnel data is only stored for the length of time that is required for company reasons and permissible in accordance with statutory and company provisions.

In accordance with paragraph 3 a i, all collected traffic data, and if required, content data is deleted after three months at the latest.

This does not apply to the data which is collected and evaluated as part of an IT security incident and in accordance with paragraph 3 a ii. This data will be deleted upon completion of the transaction processing at the latest, unless it is required as further evidence for the established facts.

d. Access authorization

Only those persons who are entrusted with the technical administration of the system are authorized to access the data. Due to their assignment in accordance with data protection (GDPR) and § 88 TKG, these people are separately under an obligation to uphold data confidentiality and telecommunications privacy.

Authorized access to the data secured by the system administrators, in the case of paragraph 3 a ii, are the employees of departments that initiated the backup (e.g.C/LS, C/AU, C/IP, Head of Division) and those appointed by this third party.

The individual employee is held responsible for violations of the law. The employee shall indemnify the company from any third party claims that may be made against the company for violating rights of the private use of communication media.

Violating the provisions of these terms and conditions may have civil or criminal, as well as employment law, consequences. Furthermore, a violation can trigger a civil liability case for damages.

I hereby agree to the above terms and conditions for the private use of company communication media and agree to adhere to the terms and conditions of use.
By signing the terms and conditions of use, I declare my consent to the recording and evaluation, in accordance with paragraph 3 of these terms and conditions, including within the scope of private use. In this respect, I consent to a restriction of telecommunications privacy in accordance with § 88 TKG.

16.05.2022, Oays DARWISH, IOB/PAC

Date, Name of Employee, Department | Signature