Agreement on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR).

AS OF NOVEMBRER 11, 2022

CONCLUDED BY AND BETWEEN

– HEREINAFTER, "COMPANY" –

AND

Kyberio GmbH
Am Mittelfelde 29
30519 Hannover
Deutschland

– HEREINAFTER, "SUPPLIER" –

Preamble

This annex details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, and described in detail in agreements, contracts between the parties, or orders that the Company placed for the provisioning of services to the Supplier. Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Supplier's employees or agents process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing"). Be it noted that the processing of personal data is not the focus of the actual service provided by the Supplier. However, the possibility cannot be ruled out that through the provided services the Supplier may have technical access to personal data of the Company. Additionally, it may be possible, that within the provided service level personal data of the Company may be accessible implicitly (e.g., within the scope of a data backup process provided by the Supplier). The following provisions of this agreement govern the handling of such data.

§ 1 Scope, duration, and specification of contract processing of Data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. In particular, the Supplier's staff may come into contact with the Company's personal data within the scope of the following processes and tasks. The service agreement(s) define if, and to which extent, the Supplier performs the following service tasks:

□ **Managed Services**

The Supplier performs by order of the Company maintenance and service works on the Company's IT systems. The Supplier accesses the Company's IT systems via an encrypted network connection for the execution of the maintenance and service works. The possibility cannot be ruled out that personal data hosted on the system may become accessible to the Supplier.

□ Managed Backup

The Supplier implements a data backup process by order of the Company. For this purpose, the Supplier sets up a periodic backup according to customer specification as instructed by the Company with regards to frequency, scope, and retention period, which may include personal data. The supplier shall perform a data restore from the existing data backups at the demand of the Company. The Supplier shall also remove data from the existing data backups at the explicit order of the Company.

□ Shared Hosting

The Supplier provides the Company a web hosting environment for the operation of the Company's applications. For this purpose, the Supplier performs maintenance and service works on the environment's IT systems, as necessary. The possibility cannot be ruled out, that the Supplier may have access to personal data hosted on the systems.

□ Domain Name Administration

For the performance of necessary activities for the administration of domain names, the Supplier provides a web interface to the Company, to administrate the domains that the Company has ordered from the Supplier. This web interface collects personal data within the scope of the administration process. Extent and type of the personal data collected, are specified by the individual registrars of the ordered Top Level Domain Names and are utilized by the Supplier for the sole purpose of the registration and operation of the domain name(s). As a rule, the personal data maintained in the Supplier's system are forwarded to the individual registrar and, if applicable, to intermediary service providers for the registration and maintenance of the Domain Name(s). The forwarding of this personal data takes place after the explicit order of the Company.

□ Colocation / Remote Hands

Within the scope of colocation and remote hands services performed by the Supplier, the Supplier may receive temporary access to the Company's IT systems ("remote hands"). This temporary access may be required, e.g., for fault analysis or troubleshooting and is granted explicitly by the Company to the Supplier for the fulfillment of the remote hands process. It cannot be ruled out, that technical access to personal data that may be hosted on the Company's IT systems is possible. The Company shall ensure that granted privileges are revoked again after the completion of the remote hands' assignment. Additionally, the Supplier may perform maintenances or other manual activities on IT systems, if ordered by the Company (e.g., installation/ removal of IT systems, repair of IT systems, installation or removal of individual components of the IT systems, particularly exchange or removal of physical data media). In doing so, the Supplier explicitly follows the Company's instructions. The Company shall thereby explicitly specify the procedure of data media installation or removal.

□ Provisioning of Virtual Servers

The Supplier provides the Company a platform for the operation of virtual servers (IaaS). Thereby, potential access to personal data from the virtualization or storage layer cannot be ruled out. The Supplier is only allowed to process containers within the scope of this service (e.g., migration of a virtual storage device to another storage system), but not view or modify data within the containers.

**Custom Processing Object(s) –
please fill in, if applicable**

In all cases, the Supplier is not allowed to deliberate access, copying, modifying, deleting, or otherwise editing personal data without prior explicit instruction from the Company, or beyond the range of services described above.

This Agreement shall be based on the last contractual relationship with the Company unless the provisions of this Annex give rise to obligations going beyond this. Should the Supplier process any personal data of the Company beyond the term of the last contractual relationship, the provisions of this Order Data Agreement shall continue to apply until the termination of the processing of personal data of the Company by the Supplier.

Within the range of services described above, possible Supplier access to the following data or types of data may not be ruled out:

□ Personal master data

□ Communication data (e.g., phone no., e-mail address)

□ Contract master data (contractual relation, product, or contractual interest)

□ Customer history

□ Account and payment data

□ Planning and control data (e.g., processing status, todos)

□ Log data (e.g., IP addresses, user names in server logs)

□ Report data (from third parties, e.g., credit agencies, or public registers)

□ Other (please fill in, if applicable):

□ Customers

□ Prospective buyers

□ Subscribers

□ Employees/staff

□ Suppliers/partners

□ Commercial agents

□ Contact persons

□ Other (please fill in, if applicable):

§ 2 Scope of application and responsibilities

(1) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this annex, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(2) Company's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or a machine-readable format (in text form*), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Company shall, without undue delay*, confirm in writing or in text form any instruction issued orally. Instructions received from the Company shall be documented in the Supplier's ticket system by receipt of a corresponding e-mail or document from the Company.

(3) The Supplier may only export data in accordance with the Company´s instructions. In doing so, the Contractor shall comply with the provisions of Chapter V (Art. 44-50) of the GDPR.

§ 3 Supplier´s obligations

(1) Except where expressly permitted by Article 28 (3) (a) of the GDPR, Supplier shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(2) Supplier shall, within Supplier's scope of responsibility, organize supplier's internal organization, so it satisfies the specific requirements of data protection. Supplier shall implement technical and organizational measures to ensure the adequate protection of Company's Data, which measures shall fulfill the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organizational measures and safeguards that ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services. The company is familiar with these technical and organizational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

(3) Supplier reserves the right to modify the measures and safeguards implemented, provided, howe ver, that the level of security shall not be less protective than initially agreed upon.

(4) To the extent necessary, the Supplier shall support the Company within the scope of its possibilities with suitable technical and organizational measures in fulfilling the requests and claims of data subjects according to Chapter III of the GDPR and in complying with the obligations outlined in Articles 33 to 36 of the GDPR. (Note: The parties may agree on a remuneration provision in the Service Agreement). The Supplier shall provide support without remuneration if no explicit remuneration provision is specified in the Service Agreement. Irrespective of the remuneration arrangement set in the service agreement, support by the Supplier shall always be provided without remuneration if the support was required due to a breach of law or a breach of contract by the Supplier.

(5) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

(6) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility. Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.

(7) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

(8) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(9) The Supplier shall ensure that it complies with its obligations under Article 32 (1) (d) of the GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of the processing.

(10) The Supplier shall correct or delete the contractual data if the Company instructs it to do so, and the scope of instructions covers this. However, suppose deletion in conformity with data protection or a corresponding data processing restriction is impossible. In that case, the Supplier shall destroy data carriers and other materials in agreement with data protection based on an individual order by the Customer or shall return these data carriers to the Company unless already agreed in the contract.

(11) Data, exclusively used data carriers, and all other materials shall be deleted after the end of the order. Upon request of the Company shall surrender such data to the Company beforehand.

(12) In case of a claim against the Company by a data subject concerning any claims according to Art. 82 DS-GVO, the Supplier undertakes to support the Customer in defending the claim to the extent of its possibilities.

(13) As a rule, the Supplier shall not export the Company's personal data for processing in third countries. However, should this be necessary in exceptional cases, e.g., at the explicit request of the Customer for the provision of specific services, this shall be done exclusively to the extent and per the instructions of the Company. In particular, the Supplier shall comply with the provisions of Chapter V (Art. 45-50).

§ 4 Company's obligations

(1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(2) Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR. (Note: The parties are free to agree upon remuneration for such support in the agreement.)

(3) Company shall notify Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

(1) Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier can correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

(1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this exhibit by appropriate measures.

(2) If inspections by the Company or an inspector commissioned by the Company are necessary in individual cases, these shall be carried out during regular business hours without undue disruption of the operational process, as a rule after notification, taking into account a reasonable lead time. The Supplier may make them dependent on signing a confidentiality agreement concerning the data of other customers and the technical and organizational measures that have been set up. Suppose the inspector commissioned by the Company is directly competitive with the Supplier. In that case, the Supplier shall have a right of objection against him. The Supplier may demand remuneration for assistance in inspecting if this is agreed in the contract.

(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subcontractors (further processors on behalf of the Company)

(1) Supplier shall use subcontractors as further processors on behalf of Company only where approved in advance by Company.

(2) A subcontractor relationship shall be subject to such consent of Supplier commissioning further supplier or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Supplier shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.

(3) The Supplier shall not pass tasks within the scope of the activities agreed in this contract to subcontractors unless mutually agreed otherwise in the service agreement.

(4) Where Supplier commissions subcontractors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontractor. In particular, the Supplier shall be responsible for ensuring compliance with the Technical and Organizational Measures provided by the Subcontractor either through regular inspections or corresponding verifiable guarantees of the Subcontractors.

§ 8 Obligations to inform, mandatory written form, choice of law

(1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.

(2) No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The preceding shall also apply to any waiver or modification of this mandatory written form.

(3) In the event of any contradictions, the provisions of this Annex on data protection shall take precedence over the provisions of the Agreement. Should individual parts of this Annex be invalid, this shall not affect the validity of the rest of the Annex.

(4) This annex is subject to the laws of Germany.

§ 9 Liability and damages

The regulations on the parties' liability contained in the Agreement shall be valid also for Contract Processing unless expressly agreed upon otherwise.

Place, Date

Signature Company

Place, Date

Signature Kyberio

Addendium

Technical and Organizational Measures in accordance with Article 32 GDPR

AS OF MAY 2, 2018

ORGANIZATION:

Kyberio GmbH
Am Mittelfelde 29
D-30519 Hannover
Germany
– Henceforth KYB –

As represented by the directors:
Florian Dierks
Simon Künzel

Preamble

KYB may, within the scope of the provision of services, come into contact with personal data. The processing of personal data, however, does not lie at the focus of the actual service provision of KYB. However, it cannot be ruled out, that within the scope of the provided services, technical access to the customers' personal may become possible by KYB. According to Article 32 GDPR, KYB shall implement appropriate technical and organizational measures, whenever personal data is processed. These measures are required to demonstrate compliance with the provisions of the data privacy laws.

KYB meets these requirements by the following measures:

1. Confidentiality according to Article 32 (1) (b) GDPR

a. Physical Access Control

Physical access to the main entrance of the KYB building as well as to all side entrances is restricted by a fence. The doors and gates of the fenced area are closed by default and can only be opened by KYB staff on site with transponders. Additionally, the main gate and the main entrance of the fenced area can be opened by KYB Network Operation Center (NOC) staff via doorbell and connected manual opening function.

All access paths to the building entrances of KYB are protected by video surveillance. The NOC staff have a 24/7 live visual display of all camera footage on screens in the NOC dedicated to that purpose.

Access ways to the building are by default closed and can only be opened from the outside with security keys. Building access is monitored around the clock by qualified staff on the central reception desk/ NOC, and each staff, customer, or supplier has to register at the central reception desk. Upon registering, visitors receive a visitor pass, which must be returned upon leaving the building. Visitors are instructed about the house rules upon visiting. Visitors have to either have the authorization to register themselves, or otherwise be authorized by persons with the appropriate authorization level to authorize others for registration. The identity of visitors has to be confirmed with a valid photo identification card. Visitors are personally escorted by staff into the building from the reception area. Organizational procedures and rules ensure that strangers should never stay or move within the building unattended.

Access to the data center footprint is protected by an access control system and unaccompanied access only possible for KYB staff. For the data center "Am Mittelfelde 29" this access control has been implemented with 2-factor-authentication. Access is logged. Access logs and video footage is checked daily by KYB staff. Outside business hours the premises are controlled by an alarm system according to VDE standard. System alerts are monitored by a security service, and a documented intervention plan is followed. Additionally, all technical premises, access paths, as well as the perimeter defense, are video surveilled. Notably, all data center footprint is video surveilled, which is additionally supported by motion sensors.

b. Logical Access Control

No unauthorized access to data processing systems is granted. Access to our electronic data processing systems through external interfaces is firewall protected. Sensitive services, which must not be accessible publicly, are protected through a VPN. Publicly accessible systems, such as e-mail and internet access are isolated from other services through appropriate segmentation. KYB operates diverse, depending on the security classification, in part physically separated networks. All systems are password-protected and only allow user-specific access. Group access is not implemented. In addition to strong password requirements on the basis of internal password guidelines, a 2-factor-authentication system is used for authentication on sensitive systems of KYB. KYB's password policy, besides defining password complexity requirements, also includes additional framework parameters, such as the mandatory password resetting within defined terms, as well as prohibiting reuse of the same password.

Access privileges to customer equipment are handled in detail according to specific customer instruction and based on the services provided by KYB. According to KYB internal policies, depending on system type and classification, failed login attempts are responded to in different appropriate manners. Along with temporary access blocking, dynamic addition of network blocking, or permanent access removal, also logging and alerting takes place.

c. Data Access Control

Access to network directories or systems on which personal data is stored is limited to persons directly associated with the implementation of services, for which these data shall be used. Each user has to authenticate themselves with personalized access data. Initial access is limited to the internal KYB network, whenever system functions and customer instructions allow. In the case of external login (VPN) into the internal network of KYB, the staff receives access to network segments relevant to his duties. In the case of external access, additionally, 2-factor-authentication is deployed. For access to customer systems and equipment, customer-specific measures are agreed on with the customer. General access paths for KYB employee access on customer systems, if pertinent to the assignment, are protected with strong encryption.

KYB staff is only granted necessary privileges, as defined for the system or application. There is a clear distinction between administrators of an application or system and additional user groups. Access privileges are checked bi-annually with regards to need and correct configuration in the context of the internal auditing process.

d. Separation Control

KYB processes proprietary personal data only within the scope of systems and processes needed for the specific assignment. Within the scope of proprietary processing of personal data, KYB separates test environments from production environments. Depending on the service provided, KYB segregates customer data either physically (separate hardware systems, e.g. "dedicated server hosting"), or logically. Logical segregation may be realized in different ways, depending on the service provided. ("virtual server," "multitenant software"). The customer is responsible for any further separation control measures for the storage and processing of personal data within the scope of the order processing.

2. Integrity according to Article 32 (1) (b) GDPR

a. Data Transfer Control

The transmission of personal or other confidential data occurs with transport encryption or higher. KYB has an internal policy concerning the use of cryptographic methods, with clear definitions about which cryptographic methods are permissible in which constellation and with which technical specifications.

KYB thereby follows the guidelines of the German Federal Office for Information Security (BSI), as well as those of the US National Institute of Standards and Technology (NIST).

Furthermore, KYB recommends the use of file-based encryption for the customer communication, whenever personal data is transferred. This way, even the temporary storage of data on KYB or the customer side is secured. This method requires, however, that the customer has the technical capacity to receive or transmit such an encrypted file. Insofar as KYB identifies this possibility with the customer, KYB will use such a method of file-based encryption, in coordination with the customer.

KYB follows a standard process for the storage, deletion, and physical destruction of data media. The data media, their safe storage location, as well as their consecutive return, deletion, or destruction, are logged accordingly. The destruction security level is H-4 according to the DIN standard 66399-2.

The shipping of personal data follows the strict conditions and safeguards provided for by law. Mobile data media with personal data are only stored in secured premises, and, if not in use, in a safe. Data which are no longer required for the provisioning of an order, e.g., blocked data, are stored in a separate, access-protected storage area. The repair and disposal of data media or hardware occur only by appropriately liable and certified companies. The same holds true for the disposal of data on paper.

b. Data Entry Control

Only selected staff may access the customer systems and data within the scope of a customer project. Thereby, only staff are selected, who are needed for the provisioning of the contractually agreed upon services. The legitimation of staff follows from the allocation to the group of staff, assigned for a particular customer. All staff has been committed to maintaining confidentiality, as well as to comply with legal requirements and internal policies.

Activities on customer systems are logged. Where technically possible, all changes and actions are automatically logged. Additionally, manual logging of activity is recorded and periodically inspected on a random basis.

The default operating instruction to staff is, not to modify or manipulate any personal data of the customer. Only at the explicit instruction of the customer any personal data on the customer systems may be modified. Exceptions are made for control processes for the administration of data (data backup, deletion of log data after a contractually agreed upon retention period, etc.), which occur within the scope of the operation of customer instances in default log files of the deployed server software, and which may also include personal data.

3. Availability and Resilience according to Article 32 (1) (b) GDPR

a. Availability Control

KYB operates two physically independent, and spatially separated data centers. The safeguarding of the availability of customer specific data is regulated in the agreement terms concerning the service level and service availability. KYB operates data backup storage in both data centers to this end, in order provide the possibility for cross-section data backup. Backup intervals are individually designed in agreement with the customer. For KYB's IT systems and data which are also required for the operation of the data center and therefore the availability of customer systems and data, a daily cross-section backup takes place, as well as an additional backup of all modified data, after the completion of works on KYB systems. Furthermore, storage systems, on which customer systems are operated, are protected from data loss using fault-tolerant RAID systems. Depending on the individual configuration agreement, however, there might be customer specific differences. The customer is responsible for electronic data processing systems which have been either rented by a third-party or are proprietary customer systems, which are collocated with KYB. A fire detection system is in use to minimize potential fire damage. A security company monitors alerts and follows a documented intervention plan in the case of an alert.

There are N+1 air conditioning units operational, and an emergency generator backs them.
Both data center locations have UPS systems, as well as an emergency power generator.

KYB performs active emergency prevention management within the scope of an active information security management system according to ISO-27001 on the basis of IT-Grundschutz. This ISMS includes, along with the continuous development of the emergency manual, the periodic performance of emergency testing. These tests occur at least bi-annually in the form of detailed simulation games. At least once a year, additionally, a so-called „black building test" is performed, to simulate a complete power outage. The performance of these exercises, as well as the findings, are recorded.

KYB monitors the availability of all systems required for the data center operation. Additionally, KYB monitors by default also the availability of customer systems. The monitoring scope for customer systems is determined by the customer during the provisioning phase and may be adjusted during the business relationship. As well as a timely alert in case of outage or malfunction of relevant systems or application, KYB can also provide evidence for the availability of a system or an application.

4. Process for regular Testing, Assessment, and Evaluation (Article 32 (1) (d); Article 25 (1) GDPR)

a. Data Protection Management

KYB operates a data protection management system. To this end, KYB has appointed a data protection officer, who maintains the data protection management system and reports directly to the management. Within the scope of the data protection management system KYB logs all procedures and actions that involve the processing of personal data in internal company procedure directories. Likewise, KYB operates an ISMS according to ISO-27001 on the basis of IT-Grundschutz and has been certified by the (German) Federal Office for Information Security (BSI) according to this standard. The certificate is re-assessed on an annual basis, and every three years a new application has to be submitted and a full audit performed. Technical organizational measures are audited on an annual basis, also within the annual certificate surveillance audit.

Within the framework of the data protection management system, KYB makes data protection impact assessments, if the need is identified. Additionally, KYB ensures, that all staff commit to compliance with confidentiality and data protection laws in writings, and renew their commitment annually. Likewise, a periodic awareness-raising and training process of all staff has been established.

b. Incident Response Management

KYB maintains within the framework of the established ISMS a documented process for incident response management. Together with escalation and reporting channels, this process also includes review and analysis, and consecutive optimization based on gained insights.

KYB deploys, both, equipment-based, as well as network-based solutions (intrusion detection, virus, and malware detection, anti-spam filters, as well as anomaly detectors) for the detection of incidents. KYB also monitors the infrastructure and customer systems with a monitoring solution with regards to outages and anomalies.

All incidents are documented in a ticketing system within the framework of the incident response management system. Both, the data protection officer (if personal data is involved), and the IT security must be included in the escalation process.

c. Data Protection by Default (Article 25 (2) GDPR)

KYB follows the principle of data minimization. Only data necessary for the specific process/context are processed and stored. The data protection officer regularly checks the appropriateness. All privileges are assigned according to the “need-to-have”-principle and must be justified. The assignment of privileges is regularly checked and questioned during the internal review process.

Storage and deletion terms are actively defined. The data protection officer monitors their observance.

d. Order Control (Outsourcing to Third-Parties)

KYB assesses (sub-) contractors within the framework of the supplier selection process, as well as during the continuous cooperation with regards to appropriate data protection and IT security processes. To this end, KYB performs a due diligence examination during the selection process of a (sub-) contractor, as well as random checks (documentation and on-site).

KYB ensures that all (sub-) contractors have contractually committed themselves to compliance with existing confidentiality obligations, as well as with data protection requirements. To this end, KYB enters a contractual agreement with regards to the handling of personal data with all (sub-) contractors.

Kyberio GmbH

– The Management –