PERSONAL DATA PROCESSING AGREEMENT FOR LYNQ CLOUD SERVICES (MES)

1. DEFINITIONS

Capitalised terms used in this document are defined in the Glossary at the end of this document.

2. BACKGROUND

2.1 **Purpose and Application**. This document ("DPA") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between LYNQ and Customer. This DPA applies to Personal Data processed by LYNQ and its Sub-processors in connection with its provision of the Cloud Service.

2.2 **Structure**. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organisational measures.

2.3 **GDPR**. LYNQ and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("GDPR"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

2.4 **Governance**. LYNQ acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorisations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use LYNQ as a Processor. Where authorisations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where LYNQ informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1 **Appropriate Technical and Organisational Measures**. LYNQ has implemented and will apply the technical and organisational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

3.2 **Changes**. LYNQ applies the technical and organisational measures set forth in Appendix 2 to LYNQ's Cloud Service. LYNQ may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

4. LYNQ OBLIGATIONS

4.1 **Instructions from Customer**. LYNQ will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. LYNQ will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or LYNQ otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, LYNQ will immediately notify Customer (email permitted).

4.2 **Processing on Legal Requirement**. LYNQ may also process Personal Data where required to do so by applicable law. In such a case, LYNQ shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3 **Personnel**. To process Personal Data, LYNQ and its Subprocessors shall only grant access to authorised personnel who have committed themselves to confidentiality. LYNQ and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4 **Cooperation**. At Customer's request, LYNQ will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding LYNQ's processing of Personal Data or any Personal Data Breach. LYNQ shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. LYNQ shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, LYNQ will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5 **Personal Data Breach Notification**. LYNQ will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. LYNQ may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by LYNQ.

4.6 **Data Protection Impact Assessment**. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, LYNQ will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications held by LYNQ as the processor or by LYNQ's subprocessors where applicable). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1 **Export and Retrieval by Customer**. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case LYNQ and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2 **Deletion**. Before the Subscription Term expires, Customer may use LYNQ's export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs LYNQ to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1 **Customer Audit**. Customer or its independent third party auditor reasonably acceptable to LYNQ (which shall not include any third party auditors who are either a competitor of LYNQ or not suitably qualified or independent) may audit LYNQ's control environment and security practices relevant to Personal Data processed by LYNQ only if:

(a) LYNQ has not provided sufficient evidence of its compliance with the technical and organisational measures that protect the production systems of the Cloud Service. ;

(b) A Personal Data Breach has occurred;

(c) An audit is formally requested by Customer's data protection authority; or

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

6.2 **Scope of Audit**. Customer shall provide at least sixty (60) days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of two business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimise repetitive audits. Customer shall provide the results of any audit to LYNQ.

6.3 **Cost of Audits**. Customer shall bear the costs of any audit unless such audit reveals a material breach by LYNQ of this DPA, then LYNQ shall bear its own expenses of an audit. If an audit determines that LYNQ has breached its obligations under the DPA, LYNQ will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1 **Permitted Use**. LYNQ is granted a general authorisation to subcontract the processing of Personal Data to Subprocessors, provided that:

(a) LYNQ shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. LYNQ shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

(b) LYNQ will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

(c) LYNQ's list of Subprocessors in place on the effective date of the Agreement is published by LYNQ or LYNQ will make it available to Customer upon request, including the name, address and role of each Subprocessor LYNQ uses to provide the Cloud Service.

7.2 **New Subprocessors**. LYNQ's use of Subprocessors is at its discretion, provided that:

(a) LYNQ will inform Customer in advance (by email or by posting on the support portal available through LYNQ Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

(b) Customer may object to such changes as set out in Section 7.3.

7.3 **Objections to New Subprocessors**.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to LYNQ. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of LYNQ's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty day period from the date of LYNQ's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect LYNQ's right to use the new Subprocessor(s) after the thirty day period.

(c) Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4 **Emergency Replacement**. LYNQ may replace a Subprocessor without advance notice where the reason for the change is outside of LYNQ's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, LYNQ will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.3 applies accordingly.

8. INTERNATIONAL PROCESSING

8.1 **Conditions for International Processing**. LYNQ shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2 **Standard Contractual Clauses**. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organisation or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) LYNQ and Customer enter into the Standard Contractual Clauses;

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by LYNQ and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by LYNQ) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when LYNQ has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 7.1(c), or a notice to Customer; and/or

(c) Other Controllers whose use of the Cloud Services has been authorised by Customer under the Agreement may also enter into Standard Contractual Clauses with LYNQ and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 8.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

8.3 **Relation of the Standard Contractual Clauses to the Agreement**. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of

doubt, where this DPA further specifies audit and subprocessor rules in sections 6 and 7, such specifications also apply in relation to the Standard Contractual Clauses.

8.4 **Governing Law of the Standard Contractual Clauses**. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

9. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

GLOSSARY

1.1 **"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; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to LYNQ be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

1.2 **"Data Centre"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as notified to Customer or otherwise agreed in an Order Form.

1.3 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by LYNQ on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

1.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

1.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

1.6 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

1.7 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorised Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by LYNQ or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

1.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.9 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

1.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).

1.11 **"Subprocessor"** means third parties engaged by LYNQ, in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

APPENDIX 1 - STANDARD CONTRACTUAL CLAUSES

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorised Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

LYNQ and its Subprocessors provide the Cloud Service that includes the following support:

LYNQ support the Cloud Service data centres remotely from locations where LYNQ and/or Subprocessor employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

LYNQ provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorised Users. LYNQ performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories

The transferred Personal Data concerns the following categories of data: name, phone numbers, e-mail address, photo, job title, time zone, IP address, system access / usage / authorisation data, company name, plus any application-specific data that Authorised Users enter into the Cloud Service.

Special Data Categories

LYNQ does not anticipate any special categories of information will be submitted by the exporter. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life. The data exporter may submit special categories of data to the Cloud Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service
- provision of Consulting Services;
- communication to Authorised Users
- storage of Personal Data in dedicated Azure Data Centres
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

APPENDIX 2 - TECHNICAL AND ORGANISATIONAL MEASURES

The following sections define LYNQ's current technical and organisational measures. LYNQ may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

Physical Access Control. Unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

With the exception of the sub processor Microsoft Corporation, LYNQ or any another other sub processor acting on their behalf, do not have physical access to premises, building or rooms where the cloud services infrastructure is located. Physical access controls are set out in Microsoft's Online Services Data Protection Addendum.

https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67

System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorisation.

Measures:

(a) Multiple authorisation levels are used when granting access to sensitive systems, including those storing and processing Personal Data.

(b) All personnel access LYNQ's systems with a unique identifier (user ID).

(c) No rights are granted without authorisation. In case personnel leaves the company, their access rights are revoked from Cloud Services.

(d) Cloud Services requires passwords to be changed on a regular basis and default passwords to be altered. Personalised user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form.

(e) The Cloud Services network is protected from the public network by firewalls and anti-virus software.

(f) LYNQ uses up–to-date anti-virus software at access points to the Cloud Services network (for e-mail accounts), as well as on all file servers and all workstations.

(g) Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to the Cloud Services network and critical infrastructure is protected by strong authentication.

Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorisation in the course of processing, use and storage.

Measures:

(a) Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. LYNQ uses authorisation concepts that document grant processes and assigned roles per account (user ID).

(b) LYNQ does not allow the installation of software that has not been approved by LYNQ.

(c) LYNQ shall promptly and in any event within ten (10) business days of the cessation or Cloud Services, delete and procure the deletion of all copies of the customer's data held by LYNQ or by any of its subprocessors.

Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorisation during transfer.

Measures:

(a) Personal Data in transfer over LYNQ internal and Cloud Services networks are encrypted.

(b) When data is transferred between LYNQ and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of the Cloud Services network.

Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from LYNQ data processing systems.

Measures:

(a) LYNQ only allows authorised personnel to access Personal Data as required in the course of their duty.

Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

(a) LYNQ uses controls and processes to monitor compliance with contracts between LYNQ and its customers, subprocessors or other service providers.

(b) All LYNQ employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of LYNQ customers and partners.

Availability Control. Personal Data will be protected against accidental or unauthorised destruction or loss.

Measures:

(a) LYNQ employs regular backup processes to provide restoration of business-critical systems as and when necessary.

(b) LYNQ Cloud Services provides Azure SQL backup retention period of 30 days with targeted Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of one (1) hour.

Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

(a) LYNQ Cloud Services provides a private and secure Customer environment that does not share infrastructure with any other Customer.

(b) Customer (including its Controllers) has access only to its own data.

(c) If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular case and used only to process that case; it is not accessed to process any other cases. This data is stored in dedicated support systems.

Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

(a) LYNQ has implemented a multi-layered defence strategy as a protection against unauthorised modifications.

(b) LYNQ uses the following to implement the control and measure sections described above:

(i) Firewalls;
(ii) Antivirus software;
(iii) Azure SQL Backup
(iv) Azure site recovery;

APPENDIX 3 – GDPR RELEVANT ARTICLES

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.	**Section of DPA**	**Document reference**
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organisational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organisational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organisational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses.