


Revision: A.00	<b>DATA PROTECTION POLICY FOR SUPPLIER</b>	
Owner: Compliance Department		

## DATA PROTECTION POLICY FOR SUPPLIER

To comply with our legal and regulatory requirements, and where the Supplier (“you”, “your”) processes personal data in connection with this Contract, UMS Skeldar (“UMS”, “we”, “us”, “our”) asks you to comply with the below instructions. In respect of personal data processed by you, we are the Controller and will comply with our obligations under data protection legislation in relation to the processing of personal data.

### 1. Your obligations as a Processor

You act as a Processor whenever you process personal data on behalf of us, and you must comply with your obligations under data protection legislation.

In particular,


- a) you must promptly notify us if you become aware of any non-compliance or risk of non-compliance with data protection legislation relating to the processing of personal data under this Contract or you become aware that you have received or are likely to receive personal data as a Processor.
- b) You must ensure that you:
  - only process personal data on our prior documented instructions and only to the extent necessary for performance of this Contract, or to the extent required by applicable law. If an applicable law requirement is placed on you to process personal data for other purposes, you must provide prior written notice to us unless this is prohibited by law;
  - promptly inform us if our instructions would be in breach of data protection legislation;
  - promptly notify us of any requests from data subjects exercising their rights under data protection legislation or other complaints or allegations from data subjects, provide full cooperation to us with handling such requests and take reasonable action necessary to minimize the impact of the request, complaint or allegation and prevent recurrence;
  - unless prohibited by applicable law, promptly notify us of any requests from a Regulator in relation to personal data or personal data processing;
  - unless prohibited by applicable law, provide assistance to us within the timescales requested to enable us to comply with our obligations under data protection legislation which may include agreeing to additional provisions or obligations proposed by us in relation to the protection and security of personal data, notifying us of any personal data breach, conducting privacy impact assessments (and any related consultations) and maintaining all documentation of processing operations; and
  - not create any copies of personal data without our prior written consent, unless required for the Products and/or Services.

### 2. Breach notification

In the event you become aware of or suspect that there a personal data breach occurred, you must:

- immediately investigate the personal data breach to seek to identify, prevent and mitigate the effects of the breach and to carry out any recovery or other action reasonably necessary to remedy the personal data breach;
- notify us in writing, without undue delay, and where feasible, within 48 hours of awareness of the known or suspected personal data breach and follow-up with a detailed description. Such notice must contain at least the following details:
  - (1) a description of the nature of the personal data breach;
  - (2) a description of the causes of the breach;
  - (3) a description of the likely consequences of the breach;

**Classification company confidentiality: Official**

Revision: A.00	<b>DATA PROTECTION POLICY FOR SUPPLIER</b>	
Owner: Compliance Department		

- (4) a description of the actions or remedial measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects; and
- (5) the name and contact details of the data protection officer or other appropriate contact point where more information can be obtained;
  - update us as often as we reasonably require in the circumstances;
  - promptly conduct, or support us in relation to, any investigation or analysis that we require;
  - promptly support us in any notification of the personal data breach to any Regulator and/or data subjects;
  - promptly implement measures proposed in the notification of the breach and any additional actions or remedial measures which we consider necessary as a result of the personal data breach; and
  - promptly notify us of any new information relating to the personal data breach and the identity of each affected data subject as soon as such information can be collected or otherwise becomes available.

Unless required by applicable law, you must not notify any Regulator of any events set out in this paragraph without our prior written consent.

### 3. Security

You must implement and maintain appropriate technical and organizational security measures to protect our data from security incidents and to preserve data security and confidentiality.

In particular, you must ensure that any person who is authorized by you to process our data (including its staff, agents, and subcontractors) shall be bound to an appropriate obligation of confidentiality (whether a contractual or statutory duty).

In respect of human resources security, you must ensure the reliability and personal integrity of all Staff who have access to your information systems or UMS data and that any Staff accessing UMS data knows their obligations and the consequences of a security incident.

You must ensure that appropriate physical and logical access control measures are implemented against unauthorized access and to detect unauthorized access.

in respect of backup and recovery management, you must:

- establish procedures to ensure the security of your information systems during disasters and other adverse situations, and periodically review the same; and
- maintain data backup and recovery processes and procedures in order to ensure availability of UMS data and operation of your information systems, in adverse situations.


### 4. Transfers

Transfer of personal data is permitted only to countries with legislation which is considered to provide an adequate level of protection, or in absence, you must have in place appropriate safeguards (e.g., standard contractual clauses) which guarantee personal data protection. Before transferring data, UMS must be informed about the transfer.

### 5. Subcontractors

If you use any Subcontractor that processes personal data, you must comply with the requirements of applicable data protection legislation. In particular, you must ask for UMS authorization and set out, with the Subcontractor, the same data protection obligations are required from us to you. You must have a contract in place that guarantees the implementation of appropriate technical and organizational measures to protect personal data.

**Classification company confidentiality: Official**

<b>Revision:</b> A.00	<b>DATA PROTECTION POLICY FOR SUPPLIER</b>	<b>Document Ref:</b> PL-CL-005 <b>Date of last Revision:</b> 2023-07-04	
<b>Owner:</b> Compliance Department			

## 6. Audit

You must make available to us all information reasonably necessary to demonstrate compliance with this Data Protection Policy and allow for and contribute to audits, including inspections from us in order to assess compliance with this Policy.

## 7. Return or deletion of data

Within three months of termination or expiry of the Contract, you must deliver all personal data relevant to the terminated or expired Contract in your possession to UMS and return all copies thereof, except that you are obliged by applicable laws to retain a copy.

## 8. Notices

You must provide the applicable version of the UMS External Staff Privacy Notice, available [here](#), to any of your employees and contractors that you employ or engage in the provision of any Products or Services to us.

## 9. Definitions

Item	Definition
Controller	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
Data Protection Impact Assessment	Assessment of the impact of the envisaged processing operations on the protection of personal data
Data subject	Any natural person whose personal data is being processed
DSR request	Data Subject Rights request raised by the data subject
Personal data	Any information relating to an identified or identifiable natural person ("data subject")
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data
Processing	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as receipt, collection, recording, storage, retrieval, consultation, disclosure, transmission, dissemination, combination, erasure or destruction
Processor	Natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller

**Classification company confidentiality: Official**