ANNEX 4

Requirements cloud providers

Risks	Create a record of the personal data you hold and how it will be processed in the cloud.
	Carry out a risk analysis before transferring the data to the cloud an do a regularly update.
Contractual safeguards (guidelines)	Details on the client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and relevant penalties.
	Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.
	Only authorised persons have access to the data; a confidentiality clause is included in the contract vis-à-vis the provider and its employees.
	The provider is obliged to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract.
	The provider notifies any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited.
	The provider is obliged to co-operate with regard to the client's right to monitor processing operations.
	The provider shall facilitate the exercise of data subjects' rights to access/correct/erase their data.
	The provider notifies the client of any data breach which affects the cloud client's data.
	The cloud provider can guarantee lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible.
	Obligation of the cloud provider to provide a list of locations in which the data may be processed.
	Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.
	The client should request logging of processing operations performed by the provider and its sub-contractors; the client should be empowered to audit such processing operations.
	The cloud client should make sure that the cloud provider ensures secure erasure and that the contract between the provider and the client contains clear provision for the erasure of personal data

GDPR data processing agreement	The cloud provider shall only process the personal data only on documented instructions from the controller, unless required to do so by law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
	The cloud provider ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
	The contract affords sufficient guarantees in terms of technical security and organizational measures and a specification of security measures that the cloud provider must comply with.
	The provider shall not engage another processor without prior written authorisation of the controller. The processor shall inform the controller of any intended changes concerning the processors, giving the controller the opportunity to object.
	The cloud provider shall impose the same data protection obligations as set out in the contract between the controller and the processor on that other sub processor.
	The cloud provider assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.
	The cloud provider assists the controller in ensuring compliance with the obligations regarding personal data breaches taking into account the nature of processing and the information available to the processor.
	The cloud provider at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services, and deletes existing copies.
	The cloud provider makes available all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
Availability	The provider provides timely and reliable access to personal data.
	The client should check whether it always has and will have access to the data (also in case of bankruptcy).
	The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a cloud service.
	The cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.
	If there was a major outage at the cloud provider how would this impact on your business?

Integrity	What audit trails are in place so the client can monitor who is accessing which data?
	How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss?
	Interference with the integrity of IT systems in the cloud can be prevented or detected by means of intrusion detection / prevention systems (IPS / IDS).
Confidentiality	How quickly will the cloud provider react if a security vulnerability is identified?
	Can the cloud provider provide an appropriate third party security assessment?
	Does this comply with an appropriate industry code of practice or other quality standard?
	Remote administration of the cloud platform should only take place via a secure communication channel.
	What are the data deletion and retention timescales? Does this include end of-life destruction?
	Will the cloud provider delete all data securely if the client decides to withdraw from the cloud in the future?
	Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication).
	Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and subcontractors.
	Only authorized persons can have access to data.
Transparency	The provider should provide any further information such as on the categories of recipients of the data, which can also include processors and sub-processors.
	The provider informs the client about all relevant issues.
	The controller has rights to monitor and the cloud provider has corresponding obligations to cooperate.
	The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.
	A general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors) are compliant with the applicable legal requirements and standards.
	The client is to be made aware of all subcontractors contributing to the provision of the respective cloud service.
	The provider informs client about the locations of all data centres personal data may be processed at.
	If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a

	data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider.
Isolation	The provider does not use its physical control over data from different clients to link personal data.
	There is adequate governance of the rights and roles for accessing personal data, which is reviewed on a regular basis. The implementation of roles with excessive privileges is avoided (e.g., no user or administrator access the entire cloud).
	The cloud provider guarantees that it will not use the personal data for other and/or own purposes and shall only process the personal data on behalf of the controller.
	The client must check whether the data is completely separated from the data of other customers of the cloud provider.
Security	The provider must ensure high quality authorization and authentication mechanisms.
	Communications between cloud provider and client as well as between data centres should be encrypted (in transit). Data at rest (in storage) is also encrypted. What key management is in place?
Security AP	There is a policy document for information security that described the measures that the provider takes to secure the processed personal data.
	All responsibilities, both at management level and at executive level, are clearly defined and invested.
	All employees of the provider (including external staff) receive suitable and regular training on the security and security procedures of the organization.
	IT facilities and equipment are physically protected against unauthorized access and against damage and malfunctions.
	There are procedures to allow authorized users to access the information systems and services they need for the performance of their tasks and to prevent unauthorized access to information systems.
	Activities that users perform with personal data are recorded in log files. The same applies to other relevant events, such as attempts to gain unauthorized access to personal data and disruptions that can lead to mutilation or loss of personal data.
	There are procedures for the timely and effective handling of security incidents and vulnerabilities in security as soon as they are reported.
	By organizing continuity management in the organization, the consequences are limited to an acceptable level, using a combination of preventive measures and remedial measures.
	The provider has developed policies for the protection and confidentiality of personal data. The policy states that personal data will only be processed on behalf of the controller.

Certifications	The cloud service provider can provide a copy of a third party audit certificate or a copy of the audit report verifying the certification. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard.
Legal	Make sure you have a written contract in place with your cloud provider.
	The cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.