Checklist: Where are you on your GDPR journey? YOUR COMPLIANCE

Here is a checklist of questions to assess the level of your compliance with the GDPR requirements:

The relevant questions	Level of implementation	
	☑ Done	❑ Planned on (date)
Stage of compliance 1: Making the action plan		
Has a **GDPR action and compliance plan** been developed?		
Does my company need to appoint a **personal data protection officer** (DPO)?		
✓ If yes, did I appoint one?		
Which entities/departments are involved in the compliance plan (inventory of business activities/procedures dealing with personal data)?		
Stage of compliance 2: Audit of the treatment of existing data		
Did I identify **the purposes and subjects of the processes and categories of personal data**?		
Is my company able to justify the **legal basis** of each processing of personal data?		
Did I define **retention periods** for personal data (and communicate them to data subjects)?		
Are all personal data collected necessary for the processing (proportionality)?		
Stage of compliance 3: Identification of risky processes and special categories of data		
Does my company perform processes that could potentially impact the privacy of the persons concerned?		
✓ Did I define decision criteria for determining the need of a **privacy impact study**? ✓ Did I define a privacy impact assessment method?		
Does my company perform processes that involve the **cross-referencing** of different categories of data or the **reuse** of data collected for another process?		
Does my company perform data **profiling** processes?		
Does my company transfer the processed data **outside the European Union**?		
Does my company use **subcontractors** who process personal data on behalf of my company (review of contracts with subcontractors and control of subcontractors' compliance with the GDPR requirements)?		
Stage of compliance 4: Implementation of procedures		
Did I incorporate elements of RGPD compliance into my company's procedures?		
Does my company have some management mechanisms in place for the collection, registration, modification and revocation of the **consent** of data subjects (when the legal basis is		

consent)?		
Did I establish procedures in order to satisfy requests for the **exercise of rights under the GDPR** (rights to access, rectify, erase data, to restrict processing, right to oblivion, right to data portability)? Do data subjects benefit from clear and understandable information at the moment of data collection?		
Does my company have mechanisms for **archiving** and **deleting** personal data?		
Did I integrate the GPDR into my company's **HR training programme**?		
Did I involve my company's **IT department** in GDPR compliance?		
✓ Did we put in place data **security** measures (protected access, pseudonymisation, encryption, secure storage and transfer, purge and archiving rules, etc.)?		
✓ Has a process for **detecting**, handling and reporting personal **data breaches** been adopted?		
Does my company's **insurance** cover the risks (penalties, damages, incidents, etc.) related to the processing of personal data?		
Stage of compliance 5: Documentation		
Did my company **document** its compliance with the GDPR?		
Is there an **exhaustive mapping** of personal data processed in my company's information system?		
Did I carry out an **impact analysis** of processes that could potentially impact the privacy of the persons concerned?		
Did I establish a **register of processing operations**?		
Did I establish a **register of data processing incidents**?		