🙂

nFADP Checklist

Project planning

□ Get well informed about the new data protection law

□ Define clear responsibilities and roles for the planning and execution of the project

□ Allocate the necessary financial and human resources

□ Identify the areas in your company that are relevant for data protection, i.e. the areas where personal data is processed

□ Identify the necessary technical and organizational measures to achieve compliance with the nFADP

□ Clarify the project process and plan the individual steps

□ Set a realistic time schedule

Processing directory

□ Create an appropriate file or download our template and check whether the mandatory fields are sufficient for your company or need to be expanded

□ Identify the departments where personal data is collected

□ Train your staff on how to fill out the Excel spreadsheet correctly and what information needs to be collected

□ Have the departments record all processing activities

□ Review the collected inventories to ensure accuracy and completeness

□ Compile the results into a single spreadsheet: Collect all the information from the different departments and merge it into one central spreadsheet

□ Implement a process for updates: determine at what intervals the spreadsheet will be updated to ensure that changes in data processing are incorporated on a regular basis. This must be done at least annually

Privacy Policy

□ Collect and document all processing activities in your company

□ Group processing activities by data category, processing purpose, processor, and retention criteria

□ Revise your privacy policy. You can also include the affected departments

□ Place references to your privacy policy on your website, in e-mails, and in apps

□ Implement a process for updates. Determine at what intervals your privacy policy will be updated to ensure that changes are incorporated regularly. At least annual updates are recommended

Data processing by third parties

□ Get an overview of all data processors with whom you share personal data

□ Use sample contracts and adapt them according to your needs, or ask the processors whether they offer their own sample contract (here is our own DPA).

□ Negotiate the exact contract content with each data processor individually.

□ Conclude the contracts and keep them: After all the details are settled, sign the DPAs and keep them safe to prove your legal compliance.

Cross-border data transfers

□ Make an overview of all your data processors abroad.

□ Create an agreement with each data processor and include the SCC.

□ Read the SCC carefully and adapt them to your context only where explicitly necessary.

□ Finalize the contracts and keep them to prove your legal compliance.

Data subject rights

□ Identify all locations in the company where personal data is stored. This should be evident from the processing directory, if you have created one

□ Make sure there is a way to export this data in a structured way

□ Develop and implement internal processes to handle requests (a separate process for requests for access, data transfer, correction or deletion of data, and revocation of consent)

□ Create sample letters for the various requests

□ Define the responsibilities for responding to requests and train the employees involved

Data security through TOMs

□ Identify a person in your company to coordinate the process of implementing the measures. This can be your data protection advisor, if your company has appointed one.

□ Based on the list of measures, identify potential vulnerabilities and risks related to data processing in your company. Also check whether the principle of privacy by default is adhered to.

□ Clarify with the relevant departments and IT specialists what measures can be taken to increase data security. On the technical side, these can include improved access controls, encryption, backups, data deletion and system updates; on the organizational side, processing regulations, training, emergency plans and documentation.

□ Create a priority list and monitor implementation.

□ Implement a process to regularly review and update TOMs to ensure they remain relevant to current threats and requirements.

Extra: E-mails

□ Make sure your CRM includes the ability to record consent for marketing messages.

□ Add a consent option for receiving marketing messages to your data forms where necessary.

□ Set up the double opt-in process for all e-mail sign-ups.

□ Ensure that the privacy policy is referenced each time data is collected.

□ Make sure your e-mails are sent from a sender address that can be written to, and that all promotional messages include sender and contact details and an unsubscribe option.

□ Enter into a data processing agreement with your e-mail service provider.

Conclusion

□ Conduct training for your staff to ensure that all employees have the necessary knowledge and skills to ensure data protection in practice.

□ Schedule regular privacy compliance reviews and updates to address changes both in your organization and in technological developments in a timely manner.