[Company] - Data protection policy (handbook)

[***Note: this is an internal policy on data protection which stipulates how your company processes personal data and provides guidelines to your personnel on how to handle personal data during the performance of their tasks***]

# Context and purpose of this handbook

In the context of your work for [Company], you may be led to store, use, modify or transmit various kinds of data.

If this data relates (directly or indirectly) to an individual who is identified or identifiable, the data will be considered **personal data** under European Union legislation in relation to data protection.

## What is personal data?

“Personal data” is a very broad concept. It covers individuals’ names, contact information, financial information, employment history, usernames, passwords, IP addresses, purchasing habits, etc. Data can remain “personal” even if there is no name in the relevant database. A list of customer purchases with a customer ID number and no associated name is still personal data if you (or someone else within [Company], perhaps even beyond) can link the customer ID to the individual’s name. Similarly, if you know a person’s age, function within a company and phone number, you know various characteristics that in combination enable you to identify the individual.

Data concerning companies can also be personal data: for instance, a representative’s e-mail address, professional phone number and work address are personal data.

## Why this handbook?

Personal data is a protected form of data in several countries and jurisdictions, notably the European Union (EU). As a result, there are rules in the EU and elsewhere on what you can do with personal data. We speak of “processing” of personal data as a way of covering any kind of (potential) use of personal data: storing, using, modifying, deleting, transmitting it, even merely giving or having access (e.g. remote access) to the data in question. In other words, **everything you do with personal data is regulated**.

We are therefore required to maintain a legally compliant data protection strategy that guarantees the rights of all people about whom you are processing personal data. Failure to comply can give rise to significant fines. For this reason, we as an organization wish to ensure that all employees involved in the processing of personal data know the do’s and don’ts in relation to personal data.

## How does this relate to my work?

There is a good chance that no matter your role and position, you process personal data as part of your daily tasks. [***GIVE EXAMPLE FOR DIVISION/TASK - e.g. for HR:*** For instance, an HR manager will be constantly accessing and modifying personal data regarding employees; similarly, a sales representative will be regularly updating customer contact details or adding new customers to our databases.]

In this handbook, we set out various guidelines about what you can and cannot do with personal data. Check based on your tasks which recommendations are the most relevant, but always bear in mind the other guidance in this document.

# Do’s & don’ts regarding personal data

Within [Company], we must ensure that we have a privacy-minded culture that allows us to provide our services in a way that is in line with the legal requirements.

By applying the following do’s and don’ts, your individual actions will help us meet this objective.

## General

* **DO:** Apply all [Company] policies and documentation that relate to your work.

*[Do any specific policies apply within the Company?]*

* **DO:** Make others aware of [Company]'s approach to data protection by referring to the appropriate policy or documentation.

*New customers and suppliers can be made aware of external policies; new personnel, the internal policies.*

* **DO:** Check the accuracy and up-to-date nature of any personal data you process.

*Never assume that personal data will be up-to-date. If you become aware of any change in relation to personal data regarding yourself as an employee, or regarding any customer or supplier, please update the relevant database(s) (or request an update).*

*[At which stage would you typically learn of any changes to data? (e.g. told directly by the data subject, change recorded in another database, …) What procedures can you have in place to update data?]*

* **DO:** Use personal data only for permitted and foreseen purposes.

*Within [Company], we collect personal data for specific purposes. This includes mainly [List the main purposes of processing of personal data within the Company, as identified through the data register exercise] The processing of the data will then only be permitted for those purposes (and compatible purposes). It is important to ensure that you stay within the bounds of those permitted purposes. For new initiatives or any processing that might go beyond, see section 2.6 below.*

* **DO:** Limit yourself to the collection and processing of only the personal data you need.

*Be aware that [Company] must be able to justify its collection and processing of all personal data, and that the data minimization principle requires [Company] to limit this to only what is necessary. Identify the kinds of personal data you actually need, and only request those (internally and externally).*

* **DO:** If you receive any query in relation to data protection, share it immediately with the [Compliance Officer] ([e-mail address]) unless otherwise directed.

*[Company] has procedures and documentation in place to respond to the most common queries, and has expert knowledge internally and externally through its advisors. Share all queries with [Company]'s [Compliance Officer] unless there already is a specific procedure that gives you the answer to provide to the individual in question.*

*[Are there any kinds of queries you have already received? If so, give examples.]*

* **DON’T:** Don’t share any personal data, even with colleagues, except to the extent necessary.

*Treat all personal data as confidential and keep it secure. Do not allow access to personal data unless you know this is necessary, and ensure personal data is not spread further. Limit the kinds of personal data shared. [Think of relevant example - e.g. for mailing campaigns, your supplier might only need your clients’ e-mail address and name, but not their postal address. Select the fields to export from your database or columns in your Excel file, and don’t do a complete database export.]*

## Special kinds of personal data

* **DO:** Check relevant procedures or contact the [Company]'s [Compliance Officer] if you are led to process any personal data regarding children, an individual’s health, race, religious beliefs, criminal history (including suspicions).

*Some categories of personal data are granted additional layers of protection, and must be treated with extra care.*

*[Can be deleted if no chance of sensitive data being processed within the division. Pay particular attention to personal data relating to criminal history.]*

## Your devices

* **DO:** [IF APPLICABLE Apply the [Company] security policies, including the information security privacy policy]. In particular, the following measures should be taken with regard to your devices:
* **DO:** Keep your passwords private and do not share them with anyone.

*Anyone can find that secret note on your desk. Limit access to other people’s data.*

* **DO:** Lock your devices (computer / phone / …) whenever you are not using them, to protect [Company] data.

*Leaving your device unlocked would allow someone else to look at your personal data but also personal data of others to which they might not have been granted access.*

*[Are there any systematic security failings within the division? Use them as an example.]*

## Contacts with suppliers / service providers

* **DO:** Only share personal data received from suppliers (internally and externally) after checking that you have the right to do so.

*[Think of examples that are telling - for instance:] E.g. if you use a third party to enrich your data (changes of address, additional categories of information, …), [Company] will still be required to inform the individuals in question of the fact that it processes additional kinds of personal data, and can rely on the supplier’s provision of this information if it has evidence of the fact that the whole information (see list in data protection legislation) has been provided.*

## Marketing

* **DO:** Ensure that you have the right to send digital commercial communications to the selected recipients including consent where needed.

*Under related rules, consent is required for dispatch of e.g. newsletters or marketing campaigns to individuals (professionals or consumers) by electronic mail (e-mail, SMS, direct message on social media, etc.), except as regards the promotion to existing customers of products/services similar to those for which they are customers.*

*[Remove if no marketing by the relevant division.]*

## New initiatives, products or services

* **DO:** Check whether the contemplated processing is already covered by existing purposes and information.

*If not, further action may be required (information to the data subject, documentation regarding the purposes, etc.). Read the [Company] policies and get in touch with the Compliance Officer in this respect.*

*[Link to a copy of the register of processing activities]*

* **DO:** Check whether you need to carry out a (full) Data Protection Impact Assessment (DPIA).

*See our DPIA tool - by using this tool, you will be able to check whether a full DPIA is required or whether you only need to provide limited information in relation to your project.*

* **DO:** If it’s a website or application, ensure the processing of personal data is covered by the [Company] [external privacy statement].

*The processing of personal data in new websites or applications might already be covered by the description in the privacy statement. If so, no specific action will be needed (except featuring a link to the privacy statement on the website or in the application). Otherwise, the statement might need to be adapted.*

*Note: specific rules apply when cookies and other local files can be created on the user’s device. Check the [Company] cookie policy in this respect. [IF APPLICABLE]*