QPMC PT, Lda
Aldeamento Turistico Pedras da Rainha
Casa da Recepcao
8800-591 Cabanas de Tavira
fred.delien@qpmc.com
+351 932 566 211

GDPR CHECKLIST

Your starting point to put your company on track for PRIVACY compliance!

Follow the 10 steps of this guide by answering all the questions and discover what you will need to address in order to become compliant with the new EU privacy regulations

Step 1 – Map your data

Making some sort of data inventory is the first and most important step in preparation of the compliance roadmap.
Try to recapitulate and document all the data that you use to run the business [1].
You can do this exercise using an Excel file for example. Doing so will allow you to prove that you have gone through this important first analysis step, in addition to adding maturity to insight of the business functions.

Answer below questions. They will assist you to gain insight about your data flows.

☐ From whom do you keep personal information?

- ☐ Customers
- ☐ Suppliers
- ☐ Personnel
- ☐ Prospects
- ☐ Other: ……

☐ What categories of personal information do you keep?

- ☐ Identity data (name, address, telephone number, …)
- ☐ Invoicing data
- ☐ Sensitive data (health, biometrics, genetics…)
- ☐ Other: ……
  ……

☐ Where does this personal information come from?

……
……

<u>Caution:</u> According to GDPR, you should only cooperate with 'safe' enterprises. It is important that you include warranty clauses in the contracts that you have with your business partners.

☐ Where do you store this information? In what database(s) and where is/are this/these database(s) located?

……
……

1 Using data to run the business => very broad sense like gathering, recording, sorting, storing, updating, changing, requesting, consulting, using, providing by means of forwarding, distributing or making available in any kind of form, combining, relating, including protecting, deleting or destroying of personal information.

☐ Who has access to this/these database(s)? What are the their functions?

……
……

Is it absolutely necessary that all these persons have access to the database? Is access to the database secured? Take the required measures to secure access to the information. These measures can be digital, but also think about the simple lock on the cupboard where some of the documents are stored.

☐ Is personal information shared with or forwarded to another enterprise? If so, within the EU or outside of the EU (cloud storage)

……
……
Caution: E.g. if you correct personal information, you will have to inform the enterprise to whom you forward the personal information of the correction you've applied.
Forwarding to enterprises outside of the EU is only possible if all the conditions and obligations for forwarding are met (a.o. art. 13.1 e); art. 14.1 f); art. 15.2; art. 30.1 e); art. 44-50; …).

☐ Why do you need to keep these personal data?

……
……
*Caution: You may only gather and keep personal data for specific, explicitely defined and **legitimate purposes**. The personal data gathered must be relevant and limited to the objectives of the processing. (see further)*

☐ How long do you keep the data?

……
……
Caution: You cannot keep personal information longer than required for the intended purposes of the processing.

The result of the above exercise will assist you in the further steps required to make your company privacy compliant. This will prove especially useful in step 9, which is dealing with the setup of the register with the description of the data processing for every individual business transaction.

Step 2 – Reflect on the legal basis to process personal information

You may only gather and process personal information when a legal basis exists (art. 6).
You therefore need to define the type of data processing you want to do and on which legal basis that can be done. Mark them below:

You process personal data because:

- ❑ the person concerned has given his **consent**;

- ❑ the processing is required for the execution of an agreement;
  - e.g. if a client places an order that you need to deliver, *then you are of course allowed to process address data from this person.*
  - *e.g.if a client pays online, then you may of course process the credit card data to receive payment.*

- ❑ the processing is necessary in order to comply with a **legal obligation**;
  - *e.g. if you are an employer, then you have to supply information about your employees to the social security*

- ❑ the processing is necessary to protect the **vital interests** of the person concerned or another person;

- ❑ the processing is necessary to fulfill a **task of common interest**;

- ❑ the processing is necessary to satisfy a **legitimate interest.**
  - *e.g. health purposes like public health, social protection, prevention of fraud, direct marketing, …*
  - *In any case there shall be an evaluation of weighing interests (consideration 47).*

Why is it so important to know all this?
Depending upon the legal basis, the rights of the person concerned can vary.
A person whose personal data have been processed based on his/her prior consent has a more powerful right to request removal of his personal data (Step 4).
The legal basis also needs to be clarified in the Privacy Policy and every time you reply to a request for personal information insight.

Step 3 – Caution for sensitive personal information

It is **forbidden** to process personal information that unveils race or ethnical origin, political opinions, religious or philosophical conviction, or union membership, in addition to processing genetic or biometric data for the purpose of unique identification of a person, or health data, or data related to a person's sexual orientation or behavior (art. 9).

A number of **exceptions** are defined below:

- ❑ In case the person has given his explicit consent**;**
- ❑ To satisfy a legal obligation;
- ❑ In protection of vital interests;
- ❑ Personal information that obviously has been made public by the person concerned;
- ❑ In case of a need to raise a legal claim or when a court acts within its jurisdiction;
- ❑ When necessary to satisfy reasons of very important general interest (proportionality towards the pursued objective needs to be warranted);
- ❑ When necessary for the purpose of preventive or occupational medicine, the medical judgment of the work capability of an employee, medical diagnoses, provision of medical care or social services;
- ❑ When required for reasons of common interest for public health;
- ❑ When necessary for reasons of archiving for common interest, scientific or historical research or statistical purposes.

Check this here for your company, tick and complete:

☐ I process sensitive data: ……
……
☐ I have the following exception(s):
……
……

The processing of personal data related to criminal convictions and illegal acts can also only happen under particular conditions (art. 10).

☐ I process personal data related to criminal convictions: ……
……

If you process the above kind of data, you should consult the national website of the Privacy Commission where you will find more information on sensitive personal data and criminal conviction. You could probably also consult an Information Security professional.

Step 4 – Do you ask for consent in a correct way?

A very important act in GDPR is requesting a person's consent. According to the rules, this consent must be voluntary, specific, well informed and unambiguous. Providing consent also always needs to be a confirming act (art. 4, 11 and art. 7).

Check this here for your company, tick and complete:

☐ I foresee a voluntary choice for the consent, whereby the person can expressly agree (an 'opt-in').

☐ I inform the person clearly of what the consent is about and for what purposes (cf. right for information).

☐ I don't deduct consent from silence, a pre-ticked box, or from no reaction to a hidden consent request in long, legalistic, terms and conditions.

☐ I foresee the possibility that the person can withdraw his/her consent at all times. Withdrawal of the consent is as easy as providing consent, e.g. clearly indicate the ways the withdrawal can be done or requested.

Also notice that is important that the act of giving consent needs to be *controllable*. I.e. you must be capable to demonstrate who, when, and how consent has been provided. You should register this information into a document.

☐ Providing consent is controllable (traceable) .

Caution: Children -13!

If you, as a company, collect and process personal information from children below the age of 13, then a parent or guardian will need to provide consent (art. 8). This obligation only applies when the processing is based on consent and when it concerns services offered by the information company.
You also need to be capable to demonstrate that you exercised reasonable effort to validate the consent.

Check this here for your company

☐ I save data from children -13 based on consent.
☐ I have a system that allows me to control whether consent has been given by a parent/guardian.

What about past consent?

You do not have to request consent again when consent, that was given in the past, complies with the new requirements. If that is not the case, you need to request consent in a correct way again.

Step 5 – Do you guarantee the rights of persons concerned?

As a company, you will need to take into account a substantial number of rights that GDPR provides to the persons concerned. Make a rigorous evaluation to find out where amendments are eventually required to be compliant. It is important to understand how you are going to react upon requests from persons that want to exercise their rights. Who will be responsible? Does that person know what to do? Is it technically feasible?

Check below whether you can (correctly) deal with these rights; tick the boxes or indicate if items are not applicable:

☐ **CHECK: Clear communication and procedures to react upon requests to exercise personal rights** (art. 12 GDPR)

All information and communication needs to be provided in a concise, transparent, understandable and easily accessible format on the one hand, and, in a clear and simple language on the other hand. If a person concerned invokes one of his/her rights, then you need to react within one month from receipt of the request. In function of the complexity of the request, the response term can be lengthened with another 2 months.

☐ **CHECK: Right for information gets applied correctly** (art. 13 and 14 GDPR)

⇨ I do not process personal data when the concerned client is not aware.
⇨ The regulation defines that the following data need to be provided to your client:
- your company name and address,
- the objective of your processing (e.g. “direct marketing”),
- existence of right of resistance at no cost,
- existence of right to consult and correct the data,
- the receivers or the categories of receivers of the data;

⇨ This obligation applies regardless of whether the data have been obtained directly from the client or indirectly.

☐ **CHECK: Right to consult the data** (art. 15 GDPR)

⇨ The person from whom you keep information has the right to consult certain information and to obtain additional information on a number of things;
⇨ I organize a free of charge copy of the processed personal data within a month (extendable with 2 months);
⇨ I have a template to reply to persons requesting insight in their information.

☐ **CHECK: Right to correct the data** (art. 16 GDPR)

⇨ The person from whom you keep information has the right to correct erroneous or incomplete personal information;
⇨ I react within a month (extendable with 2 months);

⇨ I also inform all third parties to whom the data were provided and inform the concerned person to whom the information was forwarded.

☐ **CHECK: Right to remove the data** (art. 17 GDPR)

⇨ In a number of specific cases, the person from whom you keep information has the right to be "forgotten" and removed from the database.
⇨ You can refuse a request for removal in a number of cases, such as right of freedom of speech, legal obligation to process, task of public interest or public health, public interest archiving, or scientific or historical research purposes, or initiation or exercising of legal action.
⇨ I inform all third party receivers to whom the data were provided about the removal, unless this is not possible or would require a disproportionate effort (art. 19).

☐ **CHECK: Right to restrict the data** (art. 18)

In a number of cases, the person concerned may request to restrict the scope of the processed personal information.

- The person concerned disputes the correctness of the data;
- The person concerned objects against the processing;
- In case you process the data unlawful (request for removal changed to restriction);
- You no longer need the data, but the person concerned needs the data.

I inform all third party receivers to whom the data were provided about the restriction, unless this is not possible or would require a disproportionate effort (art. 19).

☐ **CHECK: Right to transfer the data** (art. 20 GDPR)

The person whose data you keep has the right to request to transfer the personal information that he has provided to another company. This transfer needs to be free of charge, needs to happen within one month (extendable with 2 months), in a structured and commonly used electronic format. This is only possible for data that you process as a company in an automated way and it is based on consent or on an agreement.

☐ Not applicable

☐ **CHECK: Right to object to processing** (art. 21 GDPR)

The person from whom you keep data has at all times and because of his/her specific situation the right to object to the processing of his/her information (unless legally determined or when required to execute an agreement). When information is gathered for purposes of direct marketing (including the profiling related to direct marketing), the person concerned can, at no cost and without justification, object to the processing of his/her data.

❑ I inform the person concerned in any case about his/her right to object and I mention this explicitly in the privacy policy.

☐ **CHECK: Automated decision making, among which profiling** (art. 22 GDPR)

Every person from whom you keep information has the right not to be subject to completely automated decision making. This right is not applicable when the decision making process 1) is required to build or execute an agreement; 2) is legally permitted; 3) is based on explicit consent.

Step 6 – Are you prepared for leaks?

If you are confronted with a data leak (e.g. your computer system was hacked and all your information might have been stolen), you have a **reporting obligation** (either immediately or within 72 hours) as of when you identify an infringement.

a) Reporting obligation with the Privacy Commission (art. 33 GDPR)

You must inform the **Privacy Commission within 72 hours** of any infringement when that infringement is likely to constitute a risk to the rights and/or freedom of individuals. You only have to report the infringements that are likely to cause harm to the person in question. E.g. identity theft, violation of confidentiality, …

b) Reporting obligation with the persons concerned (art. 34 GDPR)

If the infringement is likely to pose a high risk to the rights and freedom of the persons concerned, they must be notified without delay. E.g. if unencrypted bank details were stolen.

The obligation to report to the persons concerned does not apply in the following cases:

- ⇨ You have already taken appropriate technical and organizational protection measures with regard to those data (e.g. encryption).
- ⇨ You have taken actions afterwards to ensure that the risk will no longer occur.
- ⇨ If the obligation to report would require disproportionate efforts. In that case you have to make a public announcement or take an equally effective equivalent measure.

c) Data required to report infringements

The notification to the Privacy Commission and the persons concerned must contain a minimum number of data; see the website of the Privacy Commission. You are also required to accurately record all violations that have occurred in a document.

Make sure you apply the following practice:

- ☐ Appoint a person responsible for checking and reporting infringements:
  ……
- ☐ Prepare a template to report infringements

Make an estimation of the risk and exposure to the rights and freedom of individuals would you lose the personal data - in whatever way - in advance. Depending on this assessment, you may or may not be preparing for a possible infringement to a greater degree. We advise you to consult your IT partner to validate the assessment.

Step 7 – Do you need a Data Protection Officer (DPO)?

The appointment of a DPO is completely new. Some companies will have to appoint a DPO, a sort of prevention advisor for privacy. It is a person with both expert and practical knowledge of privacy matters, who must assist the company in supervising the internal compliance with the GDPR (Articles 37-39).

When do you need to appoint a DPO?

There are two situations in which the GDPR compels companies to appoint a DPO:

☐ Are you mainly responsible for processing sensitive information as defined in Step 2?

☐ Are you mainly responsible for processing personal data that require regular and systematic observation on a large scale?

The latter case is rather vague as such. You must interpret this situation in a sense that you process personal information as your core business. E.g. if you do direct marketing based on personal data, or when large scale profiling is part of your business. In addition, it must be a considerable amount of personal data that you treat.

If you don't find yourself in the previous cases:

☐ Not applicable

What does such an expert exactly do?

⇨ A DPO provides information and advice on the GDPR obligations to your company.

⇨ A DPO monitors compliance with the GDPR.

⇨ A DPO is the central point of contact for data protection (for the company, for the privacy commission as well as for persons whose data have been processed).

⇨ A DPO advises the company on the mandatory risk analysis and the related results.

To whom can you assign this role?

⇨ An **existing employee** with sufficient knowledge about privacy and security. The professional tasks of the employee must be compatible with the tasks of a DPO. Under no circumstances may this lead to a conflict of interest.

⇨ An **external** DPO, e.g. a consultant, who performs this task for the required number of hours per week / month.

More information is available on the website of the Privacy Commission and in the guidelines of Working Group 29 (a European body). If you need a DPO, it is recommended that you request expert support to put you in order with the Regulation.

Step 8 - Do you need to perform a Data Protection Impact Assessment (DPIA)?

Some companies will have to perform a DPIA, a kind of safety audit, for certain processing operations.

When is a DPIA required?

There are 3 situations where the GDPR imposes DPIA:

- ☐ When you systematically assess the personal characteristics of individuals (e.g. profiling) in an automated manner and take actions based on this analysis that have legal consequences or a similar impact on these individuals (e.g. direct marketing);
- ☐ In case of large-scale processing of special categories of personal data or data relating to criminal convictions and offenses;
- ☐ In the case of systematic and large-scale monitoring of publicly accessible areas.

This assessment will not be necessary for many Small to Medium sized Enterprises.
If you are not in one of the above cases, check the box below:

- ☐ Does not apply

If the DPIA indicates that the processing of the personal data poses a high risk and if you cannot limit that high risk by measures that are reasonable in terms of available technology and the associated implementation costs, you should seek advice from the Privacy Commission and take the necessary measures to control the risk.

This obligation only applies to **high risk situations**. The assessment of a 'high risk' must always be executed in function of the types of personal data, the scope and frequency of processing (Articles 35-36). E.g. when a new technology is implemented or when a profiling operation can have a significant effect on the data subject / person concerned.

You can find more information about the DPIA on the website of the Privacy Commission or in the guidelines of Working Group 29. In case you need to perform a DPIA, you should be guided by an expert.

Step 9 – Do you keep a data processing register?

Every company that processes personal information shall keep a register of its data processing activities (art. 30).

Tick the boxes below to check if you comply with the requirements.

The data processing register contains the following information:

☐ The **name and contact information** of either the data processing responsible person, or from the representative of the data processing responsible person, and/or from the Data Protection Officer

☐ The **processing objectives**

☐ A description of the **categories of the persons concerned** at one hand and from the **categories of personal data** at the other hand

☐ The **categories of receivers** to whom the personal information is or will be provided (among other, receivers in third party countries or international organizations)

☐ If possible, the **intended term in** which the different categories of data need to be erased

☐ If possible, a general description of the **technical and organizational security measures**

☐ If applicable, **forwarding** of personal information to a third party country or an international organization, including the identification of the third party country or international organization, and, if needed, a reference to the documentation with the appropriate safeguards

Numerous templates are available from different sources to manage the company's personal data processing register.
There is no official document that needs to be used and you can freely choose to compose your own template in function of e.g. software that you'd like to use. The essentials of the base objective of the register need to be respected though: recording of a complete oversight of all the data processing activities.

Step 10 - Review your Privacy Policy and amend your contracts

Privacy Policy (art. 24.2)

This exercise is also a good opportunity to evaluate your privacy policy.

In order to be GDPR compliant, you should add a number of elements:

- ☐ The complete identity of the data processor and the way that the information will be used;
- ☐ The legal basis that is required for the processing of the information;
- ☐ The time period that you will keep the information
- ☐ Whether or not you exchange information with countries outside of the European Union;
- ☐ The possibility for the person involved to file a complaint with the Privacy Commission if he/she judges that his/her personal information is treated incorrectly;
- ☐ The rights of persons involved;
- ☐ The technical and organizational measures that are taken in order to be compliant;
- ☐ The purpose(s) for wich the information will be processed;
- ☐ …

It is important that you remain very **transparent** (See also right for information, art. 13-14). While you draft/amend your privacy policy, you should consider all individual information elements that you might need to provide to the person concerned at the moment that you request consent to process his/her personal information.
In any case you will need to ensure that the privacy policy is as condensed as possible and written in a clear and comprehensible language.

Contracts (art. 28)

All your contracts (with suppliers, employees, processors[2] …) will need to be GDPR compliant.

Under the new regulation you also need to be able to guarantee that you work with 'safe' companies. The GDPR imposes that you protect your own databases adequately in the first place. In addition, when you outsource certain activities, it is crucial to evaluate whether the safety precautions that have been defined in existing contracts are adequate in addition to GDPR compliant. Existing contracts can be extended using e.g. annexes.

Evaluate existing contracts with suppliers, subcontractors, etc. and amend as required in due time

- ☐ I ensure to always have a written agreement with appropriate safety precautions.

2 As an enterprise, you may decide to delegate work and the related processing of personal information to an external subcontractor. Those subcontractors are then called 'processors'

After going through this checklist and applying all required action items, you are normally sufficiently GDPR compliant. We strongly encourage you to properly document and store all your steps and actions.

Name: …….. Date:……..

Company:..... Signature: ……..