Instructions – how to become GDPR compliant with the GDPR policies.

# General notes

We provide you with a set of templates and tools that we believe is sufficient for a small or medium-sized organisation to achieve GDPR compliance. However, your company structure or processes, or the nature of your business might require additional documents, customisations or implementation steps. Please make an appropriate effort to adapt and customise the templates and tools in the GDPR Policies to the specifics of your organisation and your country’s national data protection legislation.

You may customise the documents and tools in the GDPR Templates and make copies, adaptations, or compilation works from these templates for internal use within the organisation with which you are affiliated or associated only. All other uses of these templates without prior written authorisation of The Ekko Group Ltd (EKKO) is prohibited by copyright law. These templates may not be sold, resold, licensed, or sublicensed in the non-customised form presented here without the prior written consent of EKKO.

EKKO provides these tools and templates “as is” without warranty of any kind either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. EKKO accepts no responsibility for inaccurate or misleading information contained within the templates. EKKO may revise these templates from time to time without notice.

For your convenience we have marked in yellow the text you need to replace. However, in most cases you will need to make some additional changes and customisations to the text, structure or contents of the templates and tools in order to achieve a better match to your company specifics.

Before you start using the policies we strongly advise you to get familiar with GDPR.

Our instructions, templates and tools do not constitute, or are not meant to constitute, advice of any kind. If you require advice in relation to any legal, IT, organisational, financial or any other matter you should consult an appropriate professional.

# Step 1 - Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR.

Your decision makers and key people should get acquainted with the main principles, rights and freedoms defined by GDPR, the role of the Data Protection Officer, the rules for data subject consent, the ways to demonstrate compliance with the endorsement of security and data practices such as encryption and pseudonymisation, the importance of data protection impact assessments. These will be the leading principles and requirements in the process of GDPR implementation.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise and implement a data protection policy. This will be the backbone of your GDPR compliance. | * Data Protection Policy (Word file) |

# Step 2 - Information you hold

# You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

# The GDPR requires you to maintain records of your processing activities. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won’t be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR’s accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy. | * Data Protection Policy (Word file) |
| 2 | Document all personal data you hold | * Registry of Personal Data (Excel file) |
| 3 | Document where personal data came from and who you share it with | * Data Maps (Excel file) * Registry of Processing Activities (Excel file) |

# Step 3 - Communicating privacy information

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the Data Protection Regulator if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy. | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data subjects access rights policy and procedure | * Data Subjects Access Rights Policy and Procedure (Word file) |
| 3 | Customise and implement a non-mandatory structured data requests form | * Data Request Form (Word file) |
| 4 | Customise and implement a privacy notice to your data subjects | * Privacy Notice (Word file) |

# Step 4 - Individuals’ rights

You should make sure you have procedures that cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

* the right to be informed;
* the right of access;
* the right to rectification;
* the right to erasure (right to be forgotten);
* the right to restrict processing;
* the right to data portability;
* the right to object; and
* the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under data protection regulation but with some significant enhancements.

The right to data portability is new. It only applies:

* to personal data an individual has provided to a controller;
* where the processing is based on the individual’s consent or for the performance of a contract; and
* when processing is carried out by automated means.

You should implement appropriate policies and procedures. You will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy. | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data subject access rights policy and procedure. | * Data Subject Access Rights Policy and Procedure (Word file) |

# Step 5 - Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

* In most cases you will not be able to charge for complying with a request.
* You will have a month to comply.
* You can refuse or charge for requests that are manifestly unfounded or excessive.
* If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy. | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data subject access rights policy and procedure. | * Data Subject Access Rights Policy and Procedure (Word file) |
| 3 | Customise and implement a data request form which data subjects can use to exercise their rights. | * Data Request Form (Word file) |

# Step 6 - Lawful basis for processing personal data

You should identify the lawful basis for your processing activity, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals’ rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR’s ‘accountability’ requirements.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Document the lawful basis for all personal data you hold | * Registry of Personal Data (Excel file) |
| 3 | Document the lawful basis for all personal data processing activities | * Registry of Processing Activities (Excel file) |

# Step 7 – Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don’t meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, preticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically ‘repaper’ or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals’ consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Document the existence of consent for all consent-based personal data you hold | * Registry of Personal Data (Excel file) |
| 3 | Document the existence of consent for all consent-based personal data processing activities | * Registry of Processing Activities (Excel file) |
| 4 | Privacy notice containing consent clauses | * Privacy Notice (Word file) |

# Step 8 – Children

You should start thinking now about whether you need to put systems in place to verify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children’s personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services (‘information society services’) to children and relies on consent to collect information about them, then you may need a parent or guardian’s consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger, then you will need to get consent from a person holding ‘parental responsibility’.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children’s data your privacy notice must be written in language that children will understand.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Document any special categories of personal data you hold | * Registry of Personal Data (Excel file) |
| 3 | Document where special categories of personal data came from and how you process them | * Registry of Processing Activities (Excel file) |

# Step 9 – Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data security policy | * Data Security Policy (Word file) |
| 3 | Customise and implement a data breach notification policy and procedure | * Data Breach Notification Policy and Procedure |

# Step 10 - Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term ‘data protection by design and by default’. It also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

* where a new technology is being deployed;
* where a profiling operation is likely to significantly affect individuals; or
* where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data security policy | * Data Security Policy (Word file) |
| 3 | Customise and implement a data protection impact assessment policy and procedure | * Data Protection Impact Assessment Policy and Procedure (Word file) |
| 4 | Customise and implement a data protection impact assessment form | * Data Protection Impact Assessment Form (Excel file) |
| 5 | Customise a data processor (your vendors) due diligence request letter | * Processor Due Diligence Letter Template (Word file) |

# Step 11 – Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation’s structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

* a public authority (except for courts acting in their judicial capacity);
* an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
* an organisation that carries out the large-scale .processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |

# Step 12 – International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your ‘main establishment’ and therefore your lead supervisory authority.

The Article 29 Working party has produced guidance on identifying a controller or processor’s lead supervisory authority.

|  |  |  |
| --- | --- | --- |
|  | You need to: | Use these templates: |
| 1 | Customise your data protection policy | * Data Protection Policy (Word file) |
| 2 | Customise and implement a data transfers policy | * Data Transfers Policy (Word file) |
| 3 | Customise and implement a standard data processing agreement with the necessary clauses | * Standard Data Processing Agreement |

Compliance checklist

After completing the above steps, please go through a final GDPR compliance checklist to verify you have done everything right and all GDPR requirements have been addressed.

# Governance

One of the first things that we need to dive into as part of the GDPR compliance checklist is to ensure that as an organisation you place data governance at the center of anything you do. Compliance has to be a serious focus for companies. Internally within the organisation, it is important to create and increase awareness of data privacy issues and create a mindset where every employee feels responsible. The key thing here is to be proactive rather than reactive.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Record keeping | Maintain records of the controller and Data Protection Officer (if applicable). Maintain categories of data, logs of transfers. Wherever possible add descriptions of possible measures taken to ensure security. | Article 30 |
| Data Protection Officer (DPO) | Establish whether the company is required to have a DPO. If the company is not required to have a DPO, you may appoint a voluntary DPO. | Article 37 |
| DPO contact details must be notified to the regulatory authority and published to the public. |
| Employee Training | Employees who handle personal data of either customers or other employees must be trained to handle it according to GDPR principles. | Article 5 |
| Policies and Procedures | There is a list that covers different policies and procedures. There is no fixed way to handle this but it should be done according to what is applicable for your business. | Article 5 |

# Privacy Notices

Privacy notices basically put emphasis on the transparency requirement of GDPR. All notices issued must be information, concise and clear. Employees and customers need to be adequately informed of all data processing activities and information must be provided.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Issue notices at the right time | Notices must be given at the time that the data is obtained from the data subject, or if the data was received from a third party, within a reasonable period after obtaining the data but at the latest within one-month | Articles 12-14 |
| Be complete and concise | Notices must be complete and provide all the required information, like the identity of the controller, purpose of processing, duration, consent, right to withdraw consent, etc. | Articles 12-14 |
| Easy to understand and comprehend | The format of the notice should be easy to read, handle and understand | Articles 12-14 |

# Fair Processing

The Fair Processing category means that in order to lawfully process personal data, the conditions of processing must be met.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Establish a legal basis for processing all the personal data that you hold | As a business, you need to be able to provide evidence that you have a legal basis to own and process personal data that you hold. Consent from the data subject, the legal obligation of the controller, and special care where data is that of a child is necessary. | Articles 5, 6, 7, 9, 10, 85 to 91 |
| Profiling | A few questions to answer here: | Articles 5, 6, 7, 9, 10, 85 to 91 |
| – Does your company carry out profiling on employees or customers? |
| – If so, does this profiling result in making a decision about the individual which would have a significant legal effect or similar on that individual e.g. refusal of credit or refused for an interview? |
| – If the answer to (b) is yes, does your Company have the consent of the individuals to this profiling? |
| Children | If your business processes personal data of children, then consider the language used for privacy notices and plan out how to obtain valid consent from parents/guardians. | Articles 5, 6, 7, 9, 10, 85 to 91 |

# Data Subject Rights

Current data subject rights require you to request access to data when you need it, rectify it or delete it. Under GDPR, it’s not just the right to access data but also provide it in a machine-readable format, also called data portability.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Data subject access right | As a company, are your employees or customers allowed to get access to their personal data processed by your company? | Article 15 |
| Do you have employees that have been trained to respond to such requests within the stimulated timeframe of 1 month? |
| Processed to allow subjects to exercise their rights | This basically understands if as a company you have the technology and processes in place to allow data subjects to exercise their rights like the right to erasure, data portability, restriction of processing, and right to object. | Article 16-21 |

# Privacy by Design and by Default

One of the major objectives of GDPR is to bring privacy consideration to the forefront of every organisation. The GDPR requires data protection requirements to be considered when new technologies are designed or on-boarded or new projects using data are being considered. You should ensure that you perform an assessment to understand the impact to privacy as you onboard new projects.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Privacy by design | The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in an effective manner. The controller is responsible to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects | Article 25 |
| Privacy by default | The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons. | Article 25 |

# International Data Export

Under the International Data Export rule of the GDPR, companies are permitted to export data within its group and third-party vendors outside the European Economic Area (EEA) if the country in which the recipient of such data is established offers an adequate level of protection.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Group companies or third-party vendors | If you use group companies or third-party vendors to process data, there must be a written contract with each one of them validating that they meet the expectations set out in Article 28. | Article 28 |
| Transferring data out of EEA | If you are exporting data outside of EEA, you need to follow an approved transfer mechanism, which includes one of the following: | Articles 44-49 |
| (a) a country which has a finding of adequacy from the European Commission(b) If it is within The Company group, are binding corporate rules in place? (c) Standard contractual clauses as approved by the European Commission(d) If the transfer is to the US, on the basis of the Privacy Shield. |
| (e) With the consent of the data subject. |
| (f) The transfer is necessary to carry out a contract with the data subject |
| (g) The transfer is in the public interest |
| (h) The transfer is necessary to establish, exercise or defend legal rights |
| (i) The transfer is necessary to protect the vital interests of a person where the data subject is physically or legally incapable of giving consent. |

# Data Security

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Appropriate security measures for personal data | [Security has to be appropriate to the likely risks to individuals if data was lost, stolen or disclosed to unauthorised people.](https://blog.appknox.com/tag/cyber-security/) | Article 32 |
| It is important to note here that the security covers both organisational as well as technical measures. Some factors to consider are: |
| • Pseudonymisation |
| • Encryption |
| • Ensuring ongoing integrity, confidentiality, availability and resiliency |
| • The ability to restore in a timely manner |
| [• Processes for testing security](https://www.appknox.com/) |

# Data Breach Procedures

As part of the new GDPR compliance checklist is a data breach notification rule. The process requires organisations to act quickly, mitigate losses and, where mandatory notification thresholds are met, notify regulators and affected data subjects.

|  |  |  |
| --- | --- | --- |
| **Actions** | **Description** | **Applicable Articles of GDPR** |
| Mandatory notification | Do you have the necessary procedures in place to report a breach within 72 hours of becoming aware of it? | Article 33 |
| The breach has to be investigated and details provided to the regulator and mitigations have to be taken to address it. |
| Notification to affected individuals | If the breach is likely to result in a high risk to the rights and freedoms of individuals, the company will need to notify the individuals affected. Only if the data is encrypted or otherwise unintelligible, then individuals will not need to be notified. | Article 34 |