

[Your Company Name]

UK GDPR Compliance Statement

|  |  |
| --- | --- |
| **DOCUMENT AUTHOR:** | [Insert Author] |
| **DOCUMENT OWNER:** | [Insert Owner] |
| **STATUS:** | [Draft/Approved] |
| **DATE CREATED:** | [Insert Date] |
| **VERSION:** | [Insert Version] |
| **LAST UPDATED:** | [Insert Date] |
| **SECURITY CLASSIFICATION:** | [High/Medium/Low] |

Document Customisation

This page *(to end of the ‘disclaimer’)* provides template guidance and ***must be removed*** from the finished version. For information on customisation, refer to the *‘Instructions’* supplied in your order.

It is important to work through the document and customise any areas to ensure that the finished template accurately reflects what your organisation does and the controls that you have in place. You should consider your regulatory and legal obligations and any standards or requirements that apply to your industry or business type when customising the content.

Template Guidance

We have provided a generic template as a starting point for you to develop your own document in this compliance area. You should review and customise the template sections thoroughly to ensure that the finished version accurately reflects your organisations’ controls and responsibilities.

This drafted template for a ***GDPR Compliance Statement*** can be customised to suit your business requirements and offers a generic template for use on a website, for submission to clients or as part of your GDPR preparation program.

Whilst many organisations’ now have a compliant data protection regime; those new to complying with the GDPR may want to add a statement to their website or to provide to their clients to demonstrate how they comply with the current legislation and regulations.

Licence Terms

Purchased documents are for use within the ordering company **only** and cannot be used, sold or transferred elsewhere without written permission from Know Your Compliance Limited. Please refer to the *‘Instructions’* document for more information on our T&C’s and licence options.

Disclaimer

Know Your Compliance Limited has created this template for you to use in developing and implementing your compliance program requirements. Whilst every reasonable care is taken to ensure that the content is relevant, compliant and up to date; it is **your responsibility** to ensure that the finished policy complies with any regulatory and/or legal requirements and standards.

It is important that you customise the content to suit your industry needs and business type. Know Your Compliance Limited makes no claims or guarantees about the compliance or adequacy of the content in this template and accepts no responsibility or liability for any loss, damage or expense incurred as a result of reliance on the content contained herein. If you are unsure of your regulatory or legal obligations, you should obtain legal or professional advice before publishing, using or relying upon your finished policy.

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VERSION** | **REVISION DATE** | **SECTION REVISED** | **REASON FOR REVISION** | **DESCRIPTION OF REVISION** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Sample UK GDPR Compliance Statement**

**Introduction**

The ***United Kingdom General Data Protection Regulation (“UK GDPR”)*** applies across the UK and is based on privacy by design and taking a risk-based approach. The UK GDPR has been designed to meet the requirements of the digital age.

**Our Commitment**

**[Insert Organisation Name]** *(‘we’ or ‘us’ or ‘our’)* is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the UK GDPR *(tailored by the Data Protection Act 2018)****.***

**[Insert Organisation Name]** is dedicated to safeguarding the personal information under our remit and in developing and maintaining a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the relevant data protection new regulations and Acts.

**How We Comply with the UK GDPR**

**[This is where you should provide an overview of what measures you have implemented and maintain to become and remain UK GDPR compliant. This will differ slightly from business to business; however, we have given some examples below. You can customise/reduce the below to suit your needs.]**

**[Insert Organisation Name]** already have a consistent level of data protection and security across our organisation, with emphasis on being compliant with the UK GDPR and Data Protection Act 2018. ***Our program includes: -***

* ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
* ***Policies & Procedures* - [revising/implementing new]** data protection policies and procedures to meet the requirements and standards of the UK GDPR and any relevant data protection laws, including: -
  + ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the UK GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.
  + ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *‘data minimisation’* and *‘storage limitation’* principles and that personal information is stored, archived, and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *‘Right to Erasure’* obligation and are aware of when this and other data subject’s rights apply, along with any exemptions, response timeframes and notification responsibilities.
  + ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate, and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
  + ***International Data Transfers & Third-Party Disclosures*** – where **[insert organisation name]** stores or transfers personal information outside the UK, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules, standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
  + ***Subject Access Request (SAR)*** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent, and adequate.
* ***Legal Basis for Processing*** - we review all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the UK GDPR and Schedule 1 of the Data Protection Act 2018 are met.
* ***Privacy Notice/Policy*** – our Privacy Notice(s) comply with the UK GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
* ***Obtaining Consent*** – we have reviewed and implemented consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
* ***Direct Marketing*** – our wording and processes for direct marketing include clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
* ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing, or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the UK GDPR’s Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
* ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e., Payroll, Recruitment, Hosting etc*), we use Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our UK GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the UK GDPR.
* ***Special Categories Data* -** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Act 2018 Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

**Data Subject Rights**

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via **[our website, in the office, during induction etc]** of an individual’s right to access any personal information that **[Insert Organisation Name]** processes about them and to request information about: -

* What personal data we hold about them
* The purposes of the processing
* The categories of personal data concerned
* The recipients to whom the personal data has/will be disclosed
* How long we intend to store your personal data for
* If we did not collect the data directly from them, information about the source
* The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
* The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
* The right to lodge a complaint or seek judicial remedy and who to contact in such instances

**Information Security & Technical and Organisational Measures**

**[Insert Organisation Name]** take the privacy and security of individuals and personal information seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure, or destruction and have several layers of security measures, including: -

**[insert measures such as SSL, access controls, password policy, encryptions, pseudonymisation, practices, restriction, IT, authentication etc]**

**UK GDPR Roles and Employees**

**[Insert Organisation Name**] have designated **[insert DPO/lead name]** as our **[Data Protection Officer (DPO)/Appointed Person]**. **[Insert Organisation Name**] understands that continuous employee training, awareness and understanding is vital to the continued compliance of the UK GDPR requirements. We have a dedicated and robust employee training program specific to the data protection regulations and law and have ongoing training with existing employees, as well as session with new starters, temporary staff and those returning from absences.