

GDPR Checklist

A note for UK-based individuals and organisations:

Although the UK has left the EU, the UK Government has incorporated the provisions of the GDPR into domestic legislation as the UK GDPR. This means that the rules in this guide continue to apply equally in the UK.

|  |  |  |
| --- | --- | --- |
| 1. Basic Project Details |  |  |
| Project Name |  |  |
|  |  |  |
| Are we the **Controller** in this project?If Yes, fill in all details below |  |  |
| Are we the **Processor** in this project?If Yes, go to Section 2(c). Contracts |  |  |
| 2. Lawful Basis for Processing |  |  |
| Have we reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for the activity? |  |  |
| Which of the following is (are) the relevant basis (or bases): |  |  |
| (a) Consent |  |  |
| (b) Contract |  |  |
| (c) Legal obligation |  |  |
| (d) Vital interests |  |  |
| (e) Public task |  |  |
| (f) Legitimate interests? |  |  |
| Have we checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose? |  |  |
| Have we documented our decision on which lawful basis applies to help us demonstrate compliance? |  |  |
| Have we included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice? |  |  |
| Where we process special category data, have we also identified a condition for processing special category data, and have we documented this? |  |  |
| Where we process criminal offence data, have we also identified a condition for processing this data, and have we documented this? |  |  |
| 2(a). Consent |  |  |
| **Asking for consent** |  |  |
| Have we checked that consent is the most appropriate lawful basis for processing? |  |  |
| Have we made the request for consent prominent and separate from our terms and conditions? |  |  |
| Have we asked people positively to opt in? |  |  |
| Can we confirm that we don’t use pre-ticked boxes or any other type of default consent? |  |  |
| Do we use clear, plain language that is easy to understand? |  |  |
| Do we specify why we want the data and what we’re going to do with it? |  |  |
| Do we give individual (‘granular’) options to consent separately to different purposes and types of processing? |  |  |
| Do we name our organisation and any third party controllers who will be relying on the consent? |  |  |
| Do we tell individuals they can withdraw their consent? |  |  |
| Do we ensure that individuals can refuse to consent without detriment? |  |  |
| Do we avoid making consent a precondition of a service? |  |  |
| If we offer online services directly to children, we only seek consent if Have we age-verification measures (and parental-consent measures for younger children) in place? |  |  |
| **Recording consent** |  |  |
| Do we keep a record of when and how we got consent from the individual? |  |  |
| Do we keep a record of exactly what they were told at the time? |  |  |
| **Managing consent** |  |  |
| Do we regularly review consents to check that the relationship, the processing and the purposes have not changed? |  |  |
| Have we processes in place to refresh consent at appropriate intervals, including any parental consents? |  |  |
| Do we consider using privacy dashboards or other preference-management tools as a matter of good practice? |  |  |
| Do we make it easy for individuals to withdraw their consent at any time, and publicise how to do so? |  |  |
| Do we act on withdrawals of consent as soon as we can? |  |  |
| Can we confirm that we don’t penalise individuals who wish to withdraw consent? |  |  |
| 2(b). Legitimate Interests |  |  |
| Have we checked that legitimate interests is the most appropriate basis? |  |  |
| Do we understand our responsibility to protect the individual’s interests? |  |  |
| Have we conducted a Legitimate Interests Assessment (LIA) and kept a record of it, to ensure that we can justify our decision? |  |  |
| Have we identified the relevant legitimate interests? |  |  |
| Have we checked that the processing is necessary and there is no less intrusive way to achieve the same result? |  |  |
| Have we done a balancing test, and are confident that the individual’s interests do not override those legitimate interests? |  |  |
| Do we only use individuals’ data in ways they would reasonably expect, unless we have a very good reason? |  |  |
| Can we confirm that we are not using people’s data in ways they would find intrusive or which could cause them harm, unless we have a very good reason? |  |  |
| If we process children’s data, do we take extra care to make sure we protect their interests? |  |  |
| Have we considered safeguards to reduce the impact where possible? |  |  |
| Have we considered whether we can offer an opt-out? |  |  |
| If our Legitimate Interests Assessment (LIA) identifies a significant privacy impact, have we considered whether we also need to conduct a Data Protection Impact Assessment (DPIA)? |  |  |
| Do we keep our LIA under review, and repeat it if circumstances change? |  |  |
| Do we include information about our legitimate interests in our privacy notice? |  |  |
| **Rights related to automated decision making including profiling** |  |  |
| **All automated individual decision-making and profiling** |  |  |
| **(1) To comply with the GDPR** |  |  |
| Have we a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy? |  |  |
| Do we send individuals a link to our privacy statement when we have obtained their personal data indirectly? |  |  |
| Do we explain how people can access details of the information we used to create their profile? |  |  |
| Do we tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes? |  |  |
| Have we procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues? |  |  |
| Have we additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children)? |  |  |
| Do we only collect the minimum amount of data needed and have a clear retention policy for the profiles we create? |  |  |
| **(2) As a model of best practice** |  |  |
| Do we carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling? |  |  |
| Do we tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from? |  |  |
| Do we use anonymised data in our profiling activities? |  |  |
| **Solely automated individual decision-making, including profiling with legal or similarly significant effects (Article 22)** |  |  |
| **(1) To comply with the GDPR** |  |  |
| Do we carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to meet GDPR requirements? |  |  |
| Do we carry out processing under Article 22(1) for contractual purposes and we can demonstrate why it’s necessary? |  |  |
| ***OR*** |  |  |
| Do we carry out processing under Article 22(1) because we have the individual’s explicit consent recorded? Can we show when and how we obtained consent? We tell individuals how they can withdraw consent and have a simple way for them to do this? |  |  |
| ***OR*** |  |  |
| We carry out processing under Article 22(1) because we are authorised or required to do so? |  |  |
| Is this the most appropriate way to achieve our aims? |  |  |
| Can we confirm that we don’t use special category data in our automated decision-making systems unless we have a lawful basis to do so, and can we demonstrate what that basis is? Do we delete any special category data accidentally created? |  |  |
| Do we explain that we use automated decision-making processes, including profiling? We explain what information we use, why we use it and what the effects might be? |  |  |
| Have we a simple way for people to ask us to reconsider an automated decision? |  |  |
| Have we identified staff in our organisation who are authorised to carry out reviews and change decisions? |  |  |
| Do we regularly check our systems for accuracy and bias and feed any changes back into the design process? |  |  |
| **(2) As a model of best practice** |  |  |
| Do we use visuals to explain what information we collect/use and why this is relevant to the process? |  |  |
| Have we signed up to a set of ethical principles to build trust with our customers? Is this available on our website and on paper? |  |  |
| 2(c). Contracts |  |  |
| **Controller and processor contracts checklist** |  |  |
| ***Do our contracts include the following compulsory details:*** |  |  |
| the subject matter and duration of the processing;  |  |  |
| the nature and purpose of the processing;  |  |  |
| the type of personal data and categories of data subject;  |  |  |
| the obligations and rights of the controller? |  |  |
| ***Do our contracts include the following compulsory terms:*** |  |  |
| the processor must only act on the written instructions of the controller (unless required by law to act without such instructions); |  |  |
| the processor must ensure that people processing the data are subject to a duty of confidence;  |  |  |
| the processor must take appropriate measures to ensure the security of processing; |  |  |
| the processor must only engage a sub-processor with the prior consent of the data controller and a written contract; |  |  |
| the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR; |  |  |
| the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; |  |  |
| the processor must delete or return all personal data to the controller as requested at the end of the contract; and |  |  |
| the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state? |  |  |
| ***As a matter of good practice, do our contracts:*** |  |  |
| state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and  |  |  |
| reflect any indemnity that has been agreed? |  |  |
| **Processors’ responsibilities and liabilities checklist** |  |  |
| In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. As a processor do we: |  |  |
| only act on the written instructions of the controller (Article 29);  |  |  |
| not use a sub-processor without the prior written authorisation of the controller (Article 28.2);  |  |  |
| co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;  |  |  |
| ensure the security of our processing in accordance with Article 32;  |  |  |
| keep records of our processing activities in accordance with Article 30.2;  |  |  |
| notify any personal data breaches to the controller in accordance with Article 33;  |  |  |
| employ a data protection officer if required in accordance with Article 37; and |  |  |
| appoint (in writing) a representative within the European Union if required in accordance with Article 27? |  |  |
| As processor are we also aware that: |  |  |
| we may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR; |  |  |
| if we fail to meet our obligations, we may be subject to an administrative fine under Article 83 of the GDPR; |  |  |
| if we fail to meet our GDPR obligations we may be subject to a penalty under Article 84 of the GDPR; and |  |  |
| if we fail to meet our GDPR obligations we may have to pay compensation under Article 82 of the GDPR? |  |  |
| 3. Documentation |  |  |
| **Documentation of processing activities – requirements** |  |  |
| If we are a controller for the personal data we process, do we document all the applicable information under Article 30(1) of the GDPR? |  |  |
| If we are a processor for the personal data we process, do we document all the applicable information under Article 30(2) of the GDPR? |  |  |
| If we process special category or criminal conviction and offence data, do we document: |  |  |
| the condition for processing we rely on in the Data Protection Bill;  |  |  |
| the lawful basis for our processing; and  |  |  |
| whether we retain and erase the personal data in accordance with our policy document? |  |  |
| Do we document our processing activities in writing? |  |  |
| Do we document our processing activities in a granular way with meaningful links between the different pieces of information? |  |  |
| Do we conduct regular reviews of the personal data we process and update our documentation accordingly? |  |  |
| **Documentation of processing activities – best practice** |  |  |
| When preparing to document our processing activities do we: |  |  |
| do information audits to find out what personal data our organisation holds; |  |  |
| distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and |  |  |
| review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing? |  |  |
| As part of our record of processing activities do we document, or link to documentation, on: |  |  |
| information required for privacy notices;  |  |  |
| records of consent;  |  |  |
| controller-processor contracts;  |  |  |
| the location of personal data; |  |  |
| Data Protection Impact Assessment reports; and  |  |  |
| records of personal data breaches? |  |  |
| Do we document our processing activities in electronic form so we can add, remove and amend information easily? |  |  |

|  |  |  |
| --- | --- | --- |
| 4. Personal Data Breaches |  |  |
| **Preparing for a personal data breach** |  |  |
| Do we know how to recognise a personal data breach? |  |  |
| Do we understand that a personal data breach isn’t only about loss or theft of personal data? |  |  |
| Have we prepared a response plan for addressing any personal data breaches that occur? |  |  |
| Have we allocated responsibility for managing breaches to a dedicated person or team? |  |  |
| Do our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred? |  |  |
| **Responding to a personal data breach** |  |  |
| Have we in place a process to assess the likely risk to individuals as a result of a breach?  |  |  |
| Do we know who the relevant supervisory authority for our processing activities is? |  |  |
| Have we a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet? |  |  |
| Do we know what information we must give the ICO about a breach? |  |  |
| Have we a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms? |  |  |
| Do we know we must inform affected individuals without undue delay? |  |  |
| Do we know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects? |  |  |
| Do we document all breaches, even if they don’t all need to be reported? |  |  |

Disclaimer: This checklist is adapted from the ICO’s [Guide to the General Data Protection Regulation (GDPR)](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) and is provided for your help and guidance. It does not constitute legal advice and users should consult with their own lawyer for legal advice.