

**MAKE UK ESSENTIAL GDPR TEMPLATES FOR HR –**

**POINTS TO NOTE**

**Make UK Essential GDPR Templates for HR – Points to note**

* These ‘Points to note’ apply to the suite of Make UK Essential GDPR Templates for HR: Employee Privacy Notice, Job Applicant Privacy Notice, Data Protection Policy, Employee Record of Processing, Employee Data Retention Process, Employee Data Protection Impact Assessment, Guide to Handling a Personal Data Breach and Guide to Handling Individuals’ Requests to Exercise Data Protection Rights.
* The EU General Data Protection Regulation (**EU GDPR**) and the Data Protection Act 2018 (the **DPA 2018**) came into force on 25 May 2018. Although the UK has now left the EU, the substance of the EU GDPR has been incorporated into our domestic law and therefore continues to apply, albeit with certain modifications to take account of Brexit. This is referred to as the ‘**UK GDPR**’. In addition, the DPA 2018 continues to apply and provides further detailed rules that sit alongside and supplement the UK GDPR provisions. All of the Essential GDPR Templates for HR have been drafted to reflect the requirements of the UK GDPR and DPA 2018. We use the term ‘the GDPR’ within these templates when referring to the requirements of both the UK GDPR and the DPA 2018 together, though sometimes we need to refer to specific requirements of either the UK GDPR or the DPA 2018.
* We may occasionally refer specifically to the EU GDPR where this is necessary, for example, to draw attention to differences between the law as it applied before the UK left the EU and the current position. However, please be aware that these template documents are intended to comply with the requirements of the UK GDPR and DPA 2018. They are not intended to be suitable for use for compliance with the EU GDPR and we recommend that you take legal advice on your specific circumstances if the EU GDPR applies to your data processing activities.
* This updated version of the templates (Version 5.5) takes into account the legislation and guidance in force as at October 2023, unless otherwise stated.
* Each document is accompanied by its own key ‘Points to note’ which explains our approach and gives tips on customisation where appropriate. In order to avoid duplication, we have sought to limit detailed explanations of particular GDPR issues to the documents in which they are most relevant, but the same issues may also apply to other documents. We therefore recommend that you read all of the documents together.
* The documents generally deal with the HR-related aspects of data protection, covering the employer’s obligations in relation to personal data about Employees and Job Applicants (see below for definitions). However, note that the Data Protection Policy, the Guide to Handling a Personal Data Breach and the Guide to Handling Individuals’ Requests to Exercise Data Protection Rights all cover how the company will comply with its obligations in relation to personal data more generally (i.e. not only personal data about Employees/Job Applicants but also personal data about other individuals).
* Taking into account that the GDPR bites in all areas in which a business processes personal data, employers should not necessarily see these templates as stand-alone documents and should consider how they fit with their other HR and non-HR related GDPR documentation.
* The templates are intended to work together as a suite, or a package, of documentation (which should ease the administrative burden of managing GDPR documents). For example, assumptions we make about the categories of data processed and the processing activities tend to be carried through all the relevant documentation. Note, therefore, that when the employer tailors one of the documents in a particular way, it should check whether this also needs to be reflected in any of the other documents.
* Some of the templates cross-refer to other common policies and procedures that will include information relevant to data protection, which most employers are likely to have in place, such as an ‘Information Security Policy’, a ‘Technology and Communications Policy’, etc. The names of such policies appear in square brackets in the template documents, and will need to be tailored to reflect those in place in the employer’s organisation. Employers that do not have such policies in place may wish to consider their introduction if necessary to fill any compliance gaps. Employers that have always had such policies in place, or have had them in place for some time, may wish to review them and see whether they need to make any changes.
* All of the documents are in template form, and employers will need to adapt and customise them to the particular circumstances of their business. **This means tailoring all parts of the relevant document**, but note that, where we include square brackets, this indicates that the employer needs to make a specific choice about what to include.
* It is very important to understand that, when customising the template documents for their own business, employers must reflect the personal data they actually hold, their actual processing activities, how long they do in fact keep data for, etc. In addition, they will have to decide on the appropriate level of detail in the document.
* The template documents are usually addressed to or relate to ‘Employees’ and/or ‘Job Applicants’. These are defined terms in the templates which will encompass not just employees and job applicants in the narrow ‘employment status’ sense but also workers, contractors, agency workers, consultants, interns, volunteers, partners and directors (and applicants for all of the above positions). Employers will need to tailor the definitions of ‘Employees’ and ‘Job Applicants’ in each document so that they reflect the makeup of their workforce.
* There is, of course, no single ‘correct’ way of drafting GDPR documents, and employment and data protection lawyers produce templates that vary significantly from one another. Wherever possible, Make UK aims to keep the documentation as simple and workable as possible, taking a pragmatic approach to the difficulties thrown up by the complexities of the data protection regime and the different possible interpretations of the GDPR.
* We aim to be consistent throughout all of the template documents in our use of data protection/GDPR definitions and language. However, where possible, the language of the employee-facing documents (the Employee Privacy Notice, the Job Applicant Privacy Notice and the Data Protection Policy) is deliberately less technical, to ensure that Employees and Job Applicants understand what information is held about them and what is done with it, as required by the legislation.
* In addition, where we think it will assist people’s understanding, we have used some terms that do not appear in the GDPR. For example, the GDPR treats special category personal data differently from other personal data but does not have a particular name for this other personal data. In order to make the distinction clear, we have used the term ‘ordinary personal data’ for personal data that is not special category data. (Note that data relating to criminal offences/criminal records is not considered special category data under the UK GDPR, but in general it is included in the definition of special category data in these template documents because similar restrictions apply to its processing under the DPA 2018.) In addition, whereas the GDPR refers to the ‘lawful basis’ for processing personal data and further ‘special category conditions’ for processing special category data, our employee-facing documents refer to ‘legal grounds’ and ‘additional legal grounds’.
* Note that where we refer to the Data Protection Officer, we are referring to an official GDPR Data Protection Officer, not someone who simply has some responsibility for data protection in the organisation. Only use this term if you have appointed a Data Protection Officer within the meaning of the GDPR.
* We have presented the documents in a text/print-out format. However, they could, depending on the employer’s technological capabilities, be presented in a more user-friendly form online, e.g. using drop down boxes, links between documents, etc. Also note that in respect of certain documentation (e.g. the Employee Privacy Notice), guidance on the GDPR requires that data controllers consider the most appropriate medium, based on what the data subject will most easily be able to access.
* The template documentation aims to satisfy – in respect of HR-related data processing – the requirement in the DPA 2018 for an employer to have in place an ‘appropriate policy document’, explaining safeguards that must be put in place when processing special category personal data in certain circumstances. Having an appropriate policy document in place is required by the DPA 2018 where you are relying on special category certain lawful bases for processing, e.g. that the processing is necessary to comply with a legal obligation/exercise a legal right in relation to employment, or that the processing is necessary in the public interest for the purposes of equal opportunities monitoring. Note also that an appropriate policy document is required by the DPA 2018 if you are processing criminal offence data in reliance on the lawful basis that this is necessary for the prevention or detection of crime – as may be the case if you conduct criminal record checks during recruitment. We take the view, in accordance with ICO guidance on special category data which permits references from the ‘appropriate policy document’ to other relevant policies and procedures, that the information required in an ‘appropriate policy document’ does not need to be contained in a single document. In our template documentation, the Data Protection Policy, the Employee Record of Processing and the Employee Data Retention Process, taken together, are intended to enable you to comply with the requirement for an appropriate policy document for HR-related personal data. If you intend to use these documents as your appropriate policy document, it is especially important that you assess what you do in practice to comply with the GDPR and ensure that the content of these documents is an accurate reflection of your practices in respect of the processing of special category data.
* Remember that data protection compliance is an ongoing obligation. All of the documents that employers produce based on the GDPR template documents should be checked regularly to ensure they are still up-to-date, and should be amended if necessary.
* It is also important to bear in mind that, once customised and ready for implementation, the documents should not be presented to your Employees in isolation, but should be accompanied by appropriate training, as highlighted in the ICO’s Accountability Framework (available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/training-and-awareness/>). While in-depth training on the technicalities of the GDPR’s requirements will only be necessary for individuals who will have particular responsibility for personal data and data protection, *all* Employees should be given at least a basic level of training on key data protection concepts and the importance of data security and such training should be refreshed on a periodic basis. (Make UK can help you train your staff on data protection matters. If you would like to find out more about how we can help, or you are interested in purchasing an e-learning module to train your staff, please contact us by email to [enquiries@makeuk.org](mailto:enquiries@makeuk.org)).

**Note about the law on international transfers of personal data**

* Since the template documents are written from the perspective of a UK-based company, where relevant, they generally provide information about transfers of Employee personal data out of, rather than into, the UK (although the Data Protection Policy does refer to the possibility of the company receiving personal data from other countries).
* The template documentation reflects the fact that the UK has left the EU and that the transition period came to an end on 31 December 2020. With regard to transfers of personal data from the UK to the EEA, the UK Government has recognised the adequacy of data protection provisions in EEA countries and, with regard to transfers of personal data from the EEA to the UK, on 28 June 2021, the EU Commission formally adopted an adequacy decision in respect of the UK. The adequacy decision is valid for an initial period of four years, after which it can be renewed if the EU Commission is satisfied that the UK continues to provide an adequate level of protection for personal data. Accordingly, these template documents assume that personal data can flow freely between the UK and the EEA.
* What about transfers of personal data between the UK and other countries outside the EEA? For transfers from the UK, the position under the UK GDPR is the same as it was under the EU GDPR before the end of the transition period, i.e. such transfers are restricted unless the recipient country has an adequacy decision, other appropriate safeguards are in place such as standard contractual clauses or binding corporate rules (see below), or an exception applies.
* The UK Government has recognised the effectiveness of existing EU adequacy decisions, so companies in the UK can continue to send data freely to third parties in countries that are covered by an EU adequacy decision. (Going forwards, the UK can make its own adequacy decisions. So far, an adequacy decision has been issued in respect of the Republic of Korea (South Korea). In addition, adequacy has been confirmed in respect of organisations in the USA that have signed up to the UK Extension to the EU-US Data Privacy Framework – a binding set of commitments that are enforced in the USA by the Federal Trade Commission.)
* The safeguard most commonly relied on where the recipient country hasn’t been recognised as providing adequate protection is the use of standard contractual clauses (SCCs). You will previously have been using SCCs that were approved by the EU Commission, of which there are various different versions. However, the ICO produced a UK International Data Transfer Agreement (IDTA) to safeguard transfers of personal data outside the UK, which became available for use from 21 March 2022.
* This IDTA must be used for new transfers of personal data from the UK commencing after 21 September 2022. Alternatively, if your transfer of personal data outside the UK is part of a broader international exchange of personal data (e.g. between group companies in a multinational group) and EU SCCs are being used to comply with EU GDPR requirements, you can use a special UK Addendum to those EU SCCs, which has also been produced by the ICO. (Note that the UK Addendum is only suitable for use with the newest version of the EU SCCs, which was published in June 2021.)
* The ICO has confirmed that the old EU SCCs remain valid for contracts concluded on or before 21 September 2022 and you can continue to rely on them for existing transfers until 21 March 2024.
* From 21 March 2024, you will need to switch to the IDTA or the UK Addendum in conjunction with the new EU SCCs for any ongoing transfers of personal data out of the UK that have been reliant on the old EU SCCs.
* Another potential appropriate safeguard that companies may rely on are Binding Corporate Rules (BCRs). These are a set of written rules and procedures governing the transfer of personal data between the entities in a corporate group, that has been approved by the national data protection authority in the country where the group is established, usually where the parent company is incorporated. Where companies have existing EU-approved BCRs, the ICO will soon be able to approve a UK addendum to such BCRs provided certain conditions are met. Further information on seeking ICO approval of existing BCRs and on applying to the ICO for approval of new UK BCRs is available on the ICO website (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/>).
* Note that whenever you wish to transfer personal data to a third party in a country outside the EEA which does not have an adequacy decision, whether you propose to do so in reliance on SCCs, BCRs, or another appropriate safeguard, you will need to conduct a transfer risk assessment first. This is an assessment to establish whether, taking into account the appropriate safeguard you are intending to rely upon and the protection afforded to data subjects in the destination country, the level of protection for personal data remains equivalent to that in the UK GDPR. If it does not, you would need to take extra steps in addition to implementing your chosen appropriate safeguard. Detailed guidance on what transfer risk assessments entail is available on the ICO website (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/>).
* There are also various derogations that permit international transfers of personal data in the absence of an adequacy decision or appropriate safeguards. Most of these will not be relevant in the employment context. However, we discuss possible circumstances in which an employer might rely on one of these derogations in the ‘Points to note’ on the GDPR Template – Employee Privacy Notice.
* For transfers of personal data into the UK, it is important to be aware that other countries’ local data protection laws may impose their own restrictions. Countries which have received an adequacy decision from the EU are likely to have had to put in place their own legal restrictions on making transfers of personal data to countries outside the EEA, in order to gain and maintain the adequacy decision in their favour. Since the UK is no longer in the EEA, transfers of personal data to the UK would now be caught by such restrictions However, since the UK now benefits from an EU Commission adequacy decision itself (see above), the UK Government guidance (available online here: <https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation#receiving-personal-data-from-the-eueea-and-third-countries-which-have-eu-adequacy-decisions>) confirms that all of the other 12 countries that have EU adequacy decisions are maintaining unrestricted personal data flows with the UK. Further information is available in the ICO’s guidance on international transfers of personal data, (available online here: <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/> under the heading ‘How can we maintain transfers into the UK from countries, territories or sectors covered by an EC adequacy decision?’).

**Disclaimer**

This version of the ‘Essential GDPR Templates for HR’ suite of documents reflects the requirements of the UK GDPR and the DPA 2018, as well as Information Commissioner’s Office guidance in force as at October 2023, unless otherwise stated in the ‘Points to note’ accompanying the individual document.

The documents require customisation to accurately reflect data protection practices within your organisation. You are responsible for ensuring that you fully understand the documents and for customising them so that they are suitable for use in your organisation.

The ‘Points to note’ (and, where applicable, customisation tables) that accompany the documents are intended to provide explanations and guidance to assist you with this, but they are general in nature and do not provide a comprehensive guide to all of your GDPR obligations; they do not constitute legal advice and should not be relied upon as such.