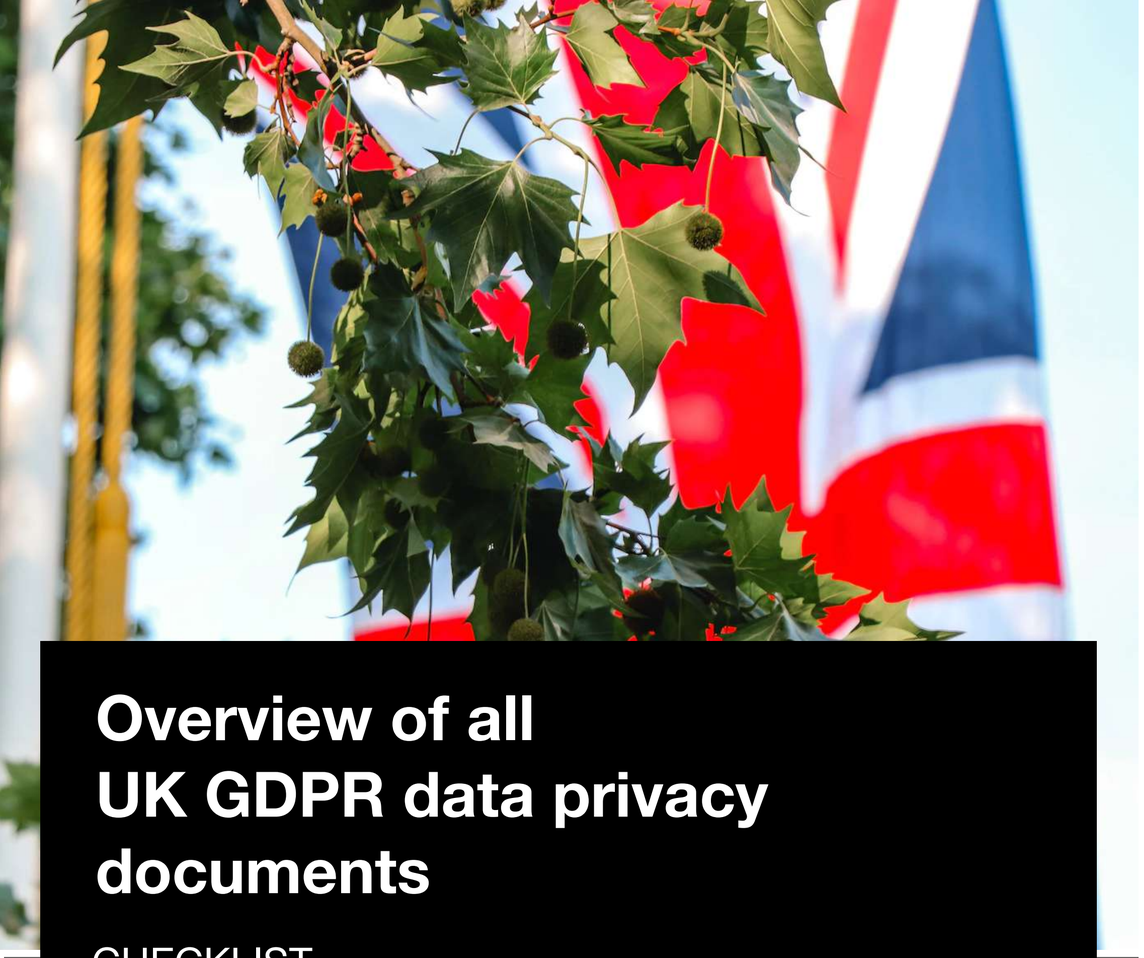
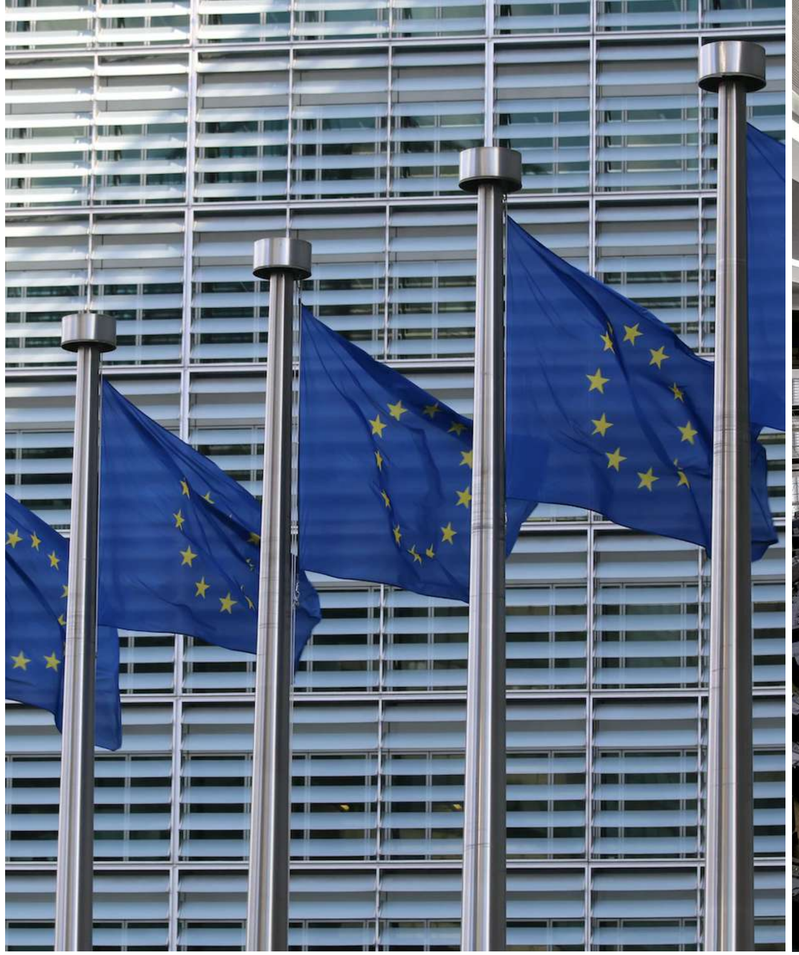
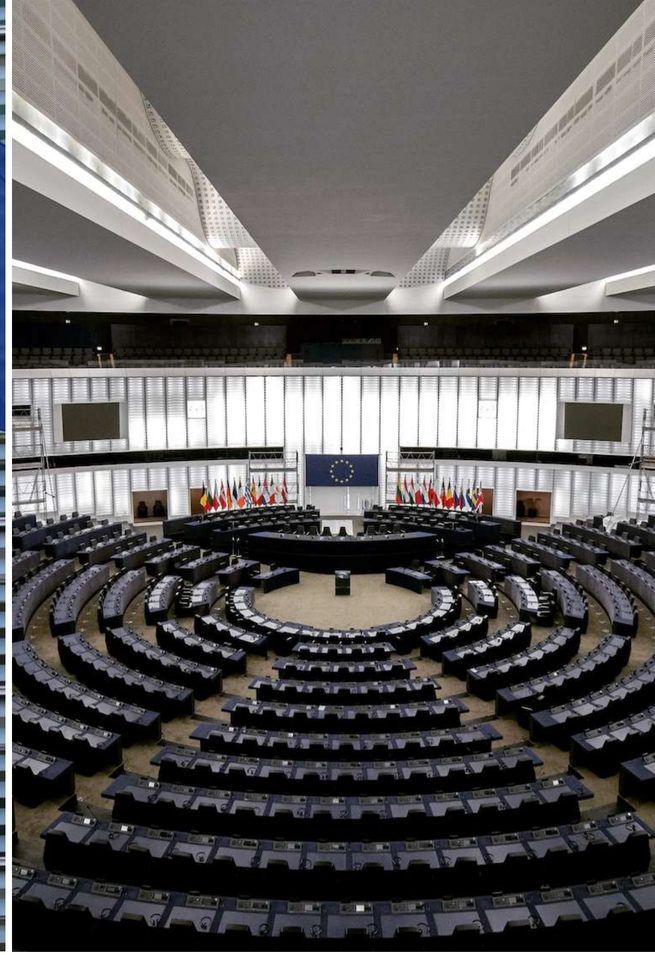






Overview of all UK GDPR data privacy documents

CHECKLIST

CW1

Accelerating Growth

Overview of the data privacy documents referred to in the UK GDPR

	What must be documented?	Legal basis	Who should prepare this documentation?	Information about the type and specific nature of the documentation
Main documentation required				
☐	Designating a data protection officer (DPO)	Art. 37 UK GDPR	All companies that appoint a data protection officer	This one-time effort (or for each re-appointment) must be documented to enable you to provide evidence. The appointment and confirmation of the DPO should therefore be in writing. The tasks of the DPO can also be precisely defined as part of the written agreement. The controller and the processor shall designate a data protection officer (DPO). While the DPO designation is done internally, the appointment must be made with the ICO.
☐	Weighing of interests	Art. 6 (1)(f) UK GDPR	Data Controller	Conducting a Legitimate Interest Assessment (LIA) helps you ensure that you can rely on the legitimate interest as a lawful basis of processing. It helps you to think clearly and sensibly about your processing and the impact it could have on the individual. As your LIA determines if the legitimate interest basis applies, you must perform it before you start processing the data and it should cover the following: tests, purpose, necessity, balancing.

☐	Deletion policy	Art. 17 UK GDPR	Any controller who carries out processing activities	An internal document/guideline that is unique for each category of personal data. A deletion policy is more important since the controller bears the burden of demonstrating and evidencing the existence of the exceptions to their obligation to delete according to Art. 17 (3) UK GDPR.
☐	Implementation of appropriate technical and organisational measures (TOMs)	Art. 24 (1), Art. 25, Art. 32 UK GDPR	Every company (both the controller and the data processor)	One-time effort: a general description of the technical and organisational measures in place constitutes part of the Directory of Processing Activities, Art. 30 (1)(g) and Art. 30 (2)(g) UK GDPR. More information can be found here.
☐	Data processing agreements	Art. 28 (3), (4) UK GDPR	Any controller who engages data processors, as well as data processors who engage sub-processors.	A data processing agreement (DPA) is a legally binding document between the controller and the processor covering details of the processing – such as its scope and purpose. It should also cover the relationship between the controller and the processor. Must be in made writing, which may also be in an electronic format.
☐	Proof of data processing instructions received from the controller, and the obligation of the employees to maintain confidentiality	Art. Art. 28 (3)(b), 29, 32 (4) UK GDPR	Companies working with controllers as data processors, data processors	Documentation of the instructions given by the controller, for each instruction given. Documentation of the employees' obligation to confidentiality – one for each new data processing contract.
☐	Records of Processing Activities	Art. 30 (1)(a – g) and (2)(a –d) UK GDPR	All companies in which data are processed (controllers and data processors). There is no obligation for companies with less than 250 employees to provide this, unless:	Must be in made writing, which may also be in an electronic format.

			• The data processing involves a risk to the rights and freedoms of the data subjects. • The data processing takes place on a regular basis. • The data processing covers special categories of data in accordance with Art. 9 UK GDPR (for example, health data, information on religion or political opinions) or data relating to criminal convictions and offences as defined in Art. 10 UK GDPR.	Contract processors should also maintain a list of the controllers and the categories of processing carried out on behalf of the controller in accordance with Art. 30 (2)(a), (b) UK GDPR.
☐	Joint controller agreement	Art. 26 UK GDPR	Companies that, as joint controllers, determine the purposes and means of processing (Examples include joint data management by several group companies, joint data processing with social media providers, fan pages).	One-time documentation effort per legal entity. This should down the distribution of responsibilities amongst the data controllers in processing the data
☐	Data protection impact assessment	Art. 35 UK GDPR	This should be carried out by companies that process data in such a way that the processing is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances, and purposes of the processing.	This should contain, at a minimum: • Description of planned processing operations and their purposes, including the legitimate interests pursued by the data controller, where appropriate. • Assessment of the necessity and proportionality of the processing operations regarding the purpose. • Assessment of the risks to the rights and freedoms of data subjects. • Remedial action to deal with the risks.

Data Privacy and third countries

☐	Data transfers to third countries, documenting adequate safeguards and assessing the circumstances of data transfers to third countries	Art. 30 (1)(e), (2)(c), Art. 49 UK GDPR	The controller companies that transfer data to third countries (outside the EU/ EEA) (e.g., through contract processors), or contract processors themselves.	Documentation as part of the Directory of Processing Activities.
☐	Appointment of a representative	Art. 3 (2), Art. 27 UK GDPR	All controllers or processors not established in the EU/EEA.	One-time documentation effort (or for each re-appointment).
☐	Proof of the existence of binding internal data protection rules - binding corporate rules (BCR)	Art. 46 (1), (2)(b), Art. 47 UK GDPR	Controller companies that operate across borders and wish to transfer data between individual members of the group of companies. The BCR then constitutes an 'adequate guarantee', e.g., if the third country does not have an adequate level of data protection.	Must be approved by the competent data protection authorities through a consistency mechanism. Please note that this can be a time-consuming process, so you must plan accordingly.

In the event of data breaches

☐	Documentation of personal data breaches	Art. 33 (1), (4), (5) UK GDPR	Controller companies that have suffered a data breach (e.g., if personal data was inadequately protected and disclosed to third parties).	The documentation must take place independently of the notification to the supervisory authority, i.e., even in the case of failure to notify, the breach must be documented with the associated facts, effects, and remedial actions taken.

☐	Proof of notification of data subjects in the event of a personal data breach	Art. 34 UK GDPR	Controllers in the event of data breaches that pose a high risk for the data subjects (e.g., disclosure of special categories of personal data to third parties).	A documentation requirement is not explicitly stated in Art. 34 UK GDPR. It is however advisable to document the circumstances of the breach in each case, as the supervisory authority may have to assess whether a) the requirements of the standard are met, and notification must therefore be made later, or b) an exception applies, and the authority determines by resolution that there is no duty to notify. In this case, we recommend that this be made in writing.
Niche cases				
☐	Proof that the data subject has reached the age of 13	Art. 8 (1), (2) UK GDPR	Providers of information society services whose users include children who have not yet reached the age of 13.	A simple checkbox does not usually suffice; more specific technologies such as video identification processes should be used.
☐	Proof of the existence of official supervision	Art. 10 UK GDPR	When processing personal data on criminal convictions, if appropriate, applicable to credit agencies or insurance companies - otherwise not of relevance.	
Documents to be provided in the event of inspection by the supervisory authority (no explicit documentation requirement, but encouraged)				
☐	Documentation of the consent obtained as well as the withdrawal of the consent given	Art. 7 (1), Art. 9 (2)(a) UK GDPR	Every company that processes personal data.	No explicit documentation requirements. Documentation is however strongly recommended, as the controller bears the burden of proof for the existence of a valid consent in cases of doubt. In the case of electronic consent, the 'double opt-in pro- cedure' is a suitable mechanism for proving that consent has been given. Obtaining consent can also be automated and continuously documented in an internal CRM system.

☐	Proof of compliance with the information requirements	Art. 12, 13, 14 UK GDPR	All companies that process personal data.	The UK GDPR does not prescribe any explicit documenta- tion requirements for the fulfilment of the information requirements. In the event of oversight by the supervisory authority, however, the requisite documents must be submitted to demonstrate compliance with data protec- tion provisions. In doing so, the written or, if applicable, electronic form must be observed as per Art. 12 (1) and (2) UK GDPR.
☐	Proof of compliance with the rights of the data subjects	Art. 15 UK GDPR	All companies, e.g., to demonstrate that the notifications made in accordance with Art. 15 to 22 UK GDPR have been complied with.	The controller must provide evidence of manifestly unfounded or excessive requests from the data subjects, Art. 12 (5)(b) UK GDPR. Otherwise, the UK GDPR does not prescribe any explicit documentation requirements for the fulfilment of the information requirements. In the event of oversight by the supervisory authority, however, the requisite documents must be submitted to demonstrate compliance with the data protection provisions. In doing so, the written or, if applicable, electronic form must be observed, Art. 12 (2) UK GDPR.
☐	Proof of the existing right to object	Art. 21 UK GDPR	The data controller and processor shall provide the necessary information to the data subjects before collecting and processing their personal data.	No specific documentation requirements, however, in the event of inspection by the supervisory authority, controllers must be able to prove that the data subjects have been advised of the right to objection. In doing so, they should observe the separate presentation of the right to object (form) referred to in Art. 21 (UK GDPR4) UK GDPR. Furthermore, they should document every objection by the data subject. In doing so, they should also document their compelling legitimate reasons in cases where the objection of the data subject is not pursued.

CW1 values: who we are

All CW1 people live by a set of values that define who we are.

Even if ex-fortune 500 consultants, we all follow the major belief of CW1 organisation. Consulting is not staffing or recruitment. Consulting is providing the best expertise to solve the most complex problems by the most expert teams in a specific field.

We are and always will be:

· People who show integrity, transparency, creativity and geniality

· People who do not care if the clock has already ticketed 100 hours this week. We strive to find solutions to problems quickly and restless.

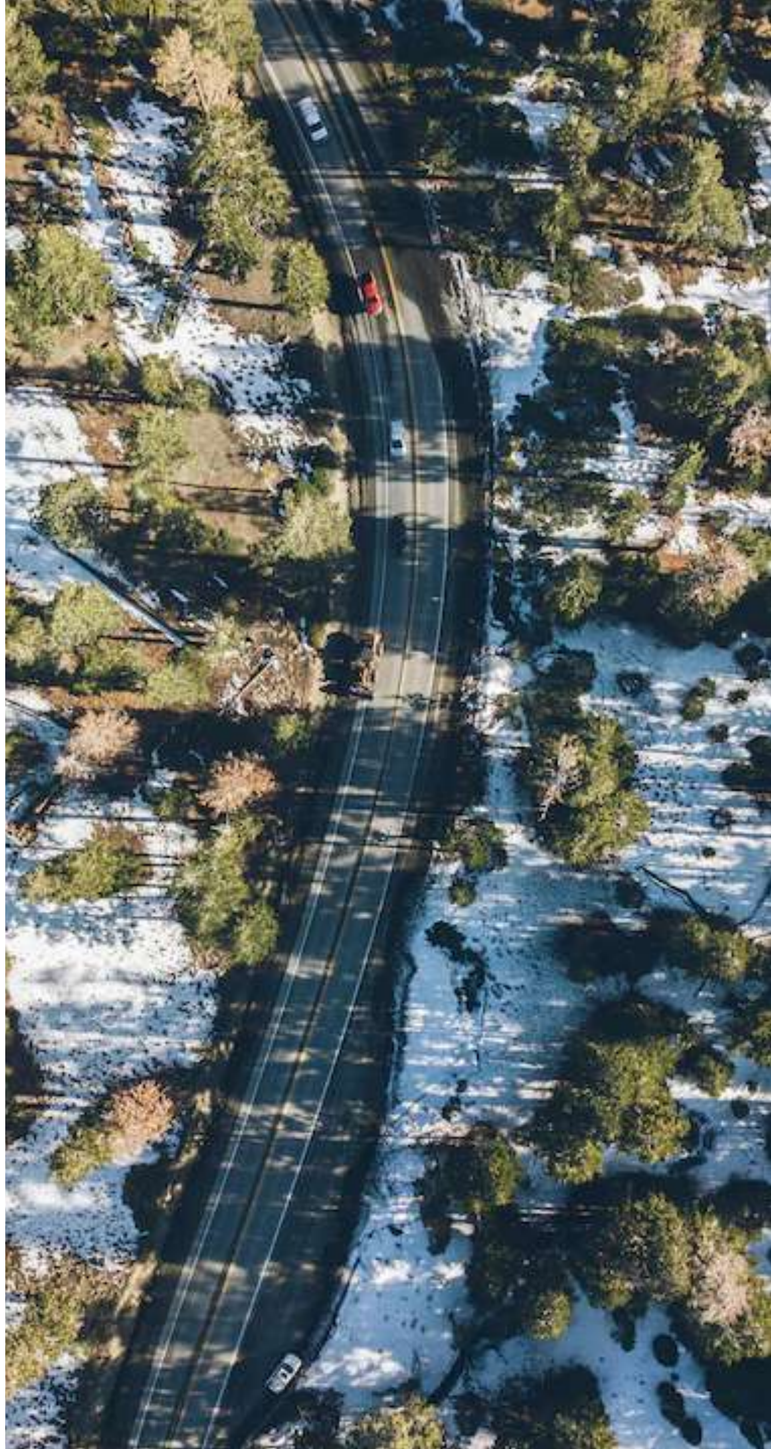
· People who care about what consulting truly is.

The CW1 purpose

CW1 is driven by one and one single purpose. To reinvent the market. All our people is focused on this rule.

We dedicate ourselves solving difficult situations that seem not having a solution. Bringing startups to their IPOs. Providing intelligence when there seems to be absolutely impossible to predict the future.

In the new world, we have already seen the whole picture - the importance of thinking globally. Through our specific programs (ESG, GCR, SAP, etc) we accelerate growth and achieve results.



About CW1

Cw1 is a multinational professional services company with engaging capabilities in Strategy, Business Intelligence, digital transformation, cloud and Data security. Combining unmatched experience and specialised skills across more than 4 industries, we offer Strategic consulting, Technology and digital services. All powered by the partnership with technology world providers such as Microsoft, Apple and IBM.

Visit us at www.cw1.com

Disclaimer

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.