

Questions	Response				question has been dealt with in the part			
	Standard answer	Expert 1	Expert 2	Expert 3	Main answer	Expert 1	Expert 2	Expert 3
Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action ?	fully modeled	fully modeled	partially modeled	fully modeled	Consent	Consent	Consent	Consent
If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual's consent to ensure compliance with the GDPR ?	fully modeled	fully modeled	fully modeled	fully modeled	Consent	Consent	Consent	Processings
Are procedures in place to demonstrate that an individual has consented to their data being processed ?	fully modeled	fully modeled	fully modeled	should not be m	Consent	Consent	Consent	_
Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data ?	fully modeled	fully modeled	fully modeled	fully modeled	Consent	Consent	Consent	Rights
Where online services are provided to a child, are procedures in place to verify age and get consent of a parent / legal guardian, where required ?	fully modeled	fully modeled	partially modeled	fully modeled	Consent	Consent	Actors	Processings
If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate ?	fully modeled	fully modeled	partially modeled	partially modele	Processings	Processings	Processings	Data
Is there a documented policy / procedure for handling Subject Access Requests (SARs) ?	fully modeled	fully modeled	partially modeled	fully modeled	Rights	Processings	Rights	Rights
Is your organisation able to respond to SARs within one month ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights	Rights	Rights	Actors
Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format ?	fully modeled	fully modeled	partially modeled	fully modeled	Rights	Rights	Rights	Actors
Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable) ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights	Rights	Rights	Actors
Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights	Rights	Rights	Actors
Are individuals told about their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest ?	fully modeled	fully modeled	fully modeled	fully modeled	Consent	Consent	Rights	Actors
Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing ?	fully modeled	fully modeled	partially modeled	fully modeled	Rights	Processings	Rights	Rights
If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected ?	fully modeled	fully modeled	not modeled	fully modeled	Consent	Consent	_	Processings
Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision ?	fully modeled	fully modeled	not modeled	fully modeled	Rights	Rights	_	Rights
Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights	Rights	Rights	Rights
Is personal data only used for the purposes for which it was originally collected ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Data	Processings	Data
Is the personal data collected limited to what is necessary for the purposes for which it is processed ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Processings	Processings	Data
Are procedures in place to ensure personal data is kept up to date and accurate and where a correction is required, the necessary changes are made without delay ?	fully modeled	fully modeled	partially modeled	fully modeled	Rights	Rights	Processings	Rights
Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Processings	Processings	Processings
Is your business subject to other rules that require a minimum retention period ?	fully modeled	fully modeled	not modeled	fully modeled	Processings	Processings	_	Processings
Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies ?	fully modeled	not modeled	fully modeled	fully modeled	Data	_	Data	Processings
Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records ?	fully modeled	fully modeled	not modeled	fully modeled	Data	Processings	_	Processings
Are service users / employees fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form using clear and plain language ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings/ consent	Processings	Processings	Rights
Where personal data is collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings / consent	Processings	Processings	Processings
If personal data is not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Article 14 of the GDPR ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings / consent	Actors	Processings	Processings
When engaging with individuals, such as when providing a service, sale of a good or CCTV monitoring, are procedures in place to proactively inform individuals of their GDPR rights ?	fully modeled	fully modeled	fully modeled	fully modeled	Consent / Rights	Rights	Rights	Consent
Is information on how the organisation facilitates individuals exercising their GDPR rights published in an easily accessible and readable format ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights / Data	Rights	Rights	Processings
Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included ?	fully modeled	fully modeled	fully modeled	partially modele	Actors	Actors	Actors	Actors
Do you need to appoint a DPO as per Article 37 of the GDPR ?	fully modeled	fully modeled	fully modeled	fully modeled	Actors	Actors	Actors	Actors
If it is decided that a DPO is not required, have you documented the reasons why ?	fully modeled	fully modeled	not modeled	fully modeled	Actors	Actors	_	Actors

Where a DPO is appointed, are escalation and reporting lines in place ? Are these procedures documented ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Actors	Actors	Processings
Have you published the contact details of your DPO to facilitate your customers / employees in making contact with them ?	fully modeled	fully modeled	fully modeled	fully modeled	Actors	Actors	Actors	Rights
If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs ? Are these procedures documented ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Actors	Processings	Processings
Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Processings	Processings	Processings
Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Processings	Processings	Processings
Is there a documented process for resolving security related complaints and issues ?	fully modeled	fully modeled	fully modeled	fully modeled	Rights	Rights	Breaches	Processings
Is there a designated individual who is responsible for preventing and investigating security breaches ?	fully modeled	fully modeled	fully modeled	fully modeled	Breaches / Actors	Breaches	Breaches	Actors
Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Actors	Data	Processings
Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained ?	fully modeled	not modeled	partially modeled	fully modeled	Data	_	Data	Processings
Can access to personal data be restored in a timely manner in the event of a physical or technical incident ?	fully modeled	fully modeled	partially modeled	fully modeled	Breaches	Breaches	Breaches	Breaches
Does the organisation have a documented privacy and security incident response plan ?	fully modeled	fully modeled	fully modeled	partially modeled	Breaches	Breaches	Breaches	Actors
Are plans and procedures regularly reviewed ?	fully modeled	fully modeled	fully modeled	partially modeled	Breaches	Breaches	Rights	Actors
Are there procedures in place to notify the office of the Data Protection Commissioner of a data breach ?	fully modeled	fully modeled	fully modeled	partially modeled	Breaches	Breaches	Breaches	Actors
Are there procedures in place to notify data subjects of a data breach (where applicable) ?	fully modeled	fully modeled	fully modeled	partially modeled	Breaches	Breaches	Breaches	Breaches
Are all data breaches fully documented ?	fully modeled	fully modeled	partially modeled	partially modeled	Breaches	Breaches	Breaches	Breaches
Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches ?	fully modeled	fully modeled	fully modeled	partially modeled	Breaches	Breaches	Breaches	Breaches
Is personal data transferred outside the EEA, e.g. to the US or other countries ?	fully modeled	fully modeled	fully modeled	fully modeled	Processings	Actors	Processings	Data
Does this include any special categories of personal data ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Actors	Processings	Data
What is the purpose(s) of the transfer ?	fully modeled	fully modeled	not modeled	fully modeled	Processings / actor	Actors	_	Processings
Who is the transfer to ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings / actor	Actors	Processings	Actors
Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is ?)	fully modeled	fully modeled	not modeled	fully modeled	Processings	Actors	_	Processings
Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Processings	Processings	Consent
Are data subjects fully informed about any intended international transfers of their personal data ?	fully modeled	fully modeled	partially modeled	fully modeled	Processings	Consent	Rights	Rights