Questionnaire	Category		Question	Key(s) word(s) of question
[8]	Personal data	Consent based data processing	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 ?	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 ?	Consent
			Are procedures in place to demonstrate that an individual has consented to their data being processed ?	Consent
			Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data ?	Withdraw consent
		Children's personal data (Article 8)	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 ?	Legal guardian/Tutor
		Legitimate interest based data processing	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 ?	legal basis
	Data subject rights	Access to personal data (Article 15)	Is there a documented policy / procedure for handling Subject Access Requests (SARs) ?	Access
			Is your organisation able to respond to SARs within one month ?	Access
		Data portability	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format ?	Portability
		Deletion and rectification	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable) ?	Rectification and forgotten
		Right to restriction of processing	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 ?	Restriction
		Right to object to processing	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 ?	Objection
			Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing ?	Objection
		Profiling and automated processing	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected ?	Automated decision making and profiling.
			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 ?	Automated decision making and profiling.
		Restrictions to data subject rights	Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted ?	Restriction
	Accuracy and retention	Purpose limitation	Is personal data only used for the purposes for which it was originally collected ?	Purpose
		Data minimisation	Is the personal data collected limited to what is necessary for the purposes for which it is processed ?	Minimisation
		Accuracy	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 ?	Accuracy
		Retention	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 ?	Retention period
		Other legal obligations governing retention	Is your business subject to other rules that require a minimum retention period ?	Retention period
			Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies ?	Retention period
		Duplication of records	Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records ?	minimisation
	Transparency requirements	Transparency to customers and employees	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 ?	Right to be informed/Transparency
			Where personal data is collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR ?	Right to be informed/Transparency
			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 ?	Right to be informed/Transparency
			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 ?	Right to be informed/Transparency
			Is information on how the organisation facilitates individuals exercising their GDPR rights published in an easily accessible and readable format ?	Right to be informed/Transparency

	Other data controller obligations	Supplier Agreements	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 ?	Third parties
		Data Protection Officers (DPOs)	Do you need to appoint a DPO as per Article 37 of the GDPR ?	DPO
			If it is decided that a DPO is not required, have you documented the reasons why ?	DPO
			Where a DPO is appointed, are escalation and reporting lines in place ? Are these procedures documented ?	DPO
			Have you published the contact details of your DPO to facilitate your customers / employees in making contact with them ?	DPO
		Data Protection Impact Assessments (DPIAs)	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 ?	DPIA
	Data security	Appropriate technical and organisational security measures	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them ?	Security
			Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data ?	Security
			Is there a documented process for resolving security related complaints and issues ?	Security
			Is there a designated individual who is responsible for preventing and investigating security breaches ?	Security Organisational question
			Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information ?	Security
			Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained ?	Security/ Retention period
			Can access to personal data be restored in a timely manner in the event of a physical or technical incident ?	Security
	Data breaches	Data Breach response obligations	Does the organisation have a documented privacy and security incident response plan ?	Breach/security
			Are plans and procedures regularly reviewed ?	Organisational question
			Are there procedures in place to notify the office of the Data Protection Commissioner of a data breach ?	Breach
			Are there procedures in place to notify data subjects of a data breach (where applicable) ?	Breach
			Are all data breaches fully documented ?	Breach
			Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches ?	Breach
	International data transfers (outside EEA)	International data transfers	Is personal data transferred outside the EEA, e.g. to the US or other countries ?	Transfer outside EU
			Does this include any special categories of personal data ?	Transfer outside EU
			What is the purpose(s) of the transfer ?	Transfer outside EU/Purpose
			Who is the transfer to ?	Transfer outside EU
			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 ?)	Transfer outside EU
		Legality of international transfers	Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented ?	Transfer outside EU
		Transparency	Are data subjects fully informed about any intended international transfers of their personal data ?	Transfer outside EU Right to be informed/Transparency
	Lawfulness, fairness and transparency	Information you hold	Your business has conducted an information audit to map data flows.	Organisational question
			Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Record of processing activities
		Lawful basis for processing personal data	Your business has identified your lawful bases for processing and documented them.	Legal basis
		Consent	Your business has reviewed how you ask for and record consent.	Consent
			Your business has systems to record and manage ongoing consent.	Consent
		Consent to process children's personal data for online services	If your business relies on consent to offer online services directly to children, you have systems in place to manage it.	Legal guardian/Tutor/ Consent

[1]		Vital interests	If you may be required to process data to protect the vital interests of an individual, your business has clearly documented the circumstances where it will be relevant. Your business documents your justification for relying on this basis and informs individuals where necessary.	Legal basis Vital interests ⊂ legal basis
		Legitimate interests	If you are relying on legitimate interests as the lawful basis for processing, your business has applied the three part test and can demonstrate you have fully considered and protected individual's rights and interests.	Legal basis Legitimate interests ⊂ legal basis
		Data Protection Fee	Your business is currently registered with the Information Commissioner's Office.	Organisational question
	Individuals' rights	Right to be informed including privacy information	Your business has provided privacy information to individuals.	Right to be informed/Transparency
		Communicate the processing of children's personal data	If your business offers online services directly to children, you communicate privacy information in a way that a child will understand	Legal guardian/Tutor
		Right of access	Your business has a process to recognise and respond to individuals' requests to access their personal data.	Access
		Right to rectification and data quality	Your business has processes to ensure that the personal data you hold remains accurate and up to date.	Rectification / Accuracy
		Right to erasure including retention and disposal	Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.	Forgotten
		Right to restrict processing	Your business has procedures to respond to an individual's request to restrict the processing of their personal data.	Restriction
		Right to data portability	Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.	Portability
		Right to object	Your business has procedures to handle an individual's objection to the processing of their personal data.	Objection
		Rights related to automated decision making including profiling	Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.	Automated decision making and profiling.
	Accountability and governance	Accountability	Your business has an appropriate data protection policy.	Security
			Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	Security
			Your business provides data protection awareness training for all staff.	Organisational question
		Processor contracts	Your business has a written contract with any processors you use.	Third parties
		Information risks	Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	DPIA Organisational question
		Data Protection by Design	Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	Security
		Data Protection Impact Assessments (DPIA)	Your business understands when you must conduct a DPIA and has processes in place to action this.	DPIA
			Your business has a DPIA framework which links to your existing risk management and project management processes.	DPIA
		Data Protection Officers (DPO)	Your business has nominated a data protection lead or Data Protection Officer (DPO).	DPO
		Management Responsibility	Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.	Organisationnelle question
	Data security, international transfers	Security policy	Your business has an information security policy supported by appropriate security measures.	Security
		Breach notification	Your business has effective processes to identify, report, manage and resolve any personal data breaches.	Breach

	transfers and breaches	International transfers	Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.	Transfer outside EU/ Security
[38]			Does your software ask and record for consent ?	Consent
			Does the consent inform the inviduals about the processing objectives ?	Purpose/ Consent
			Have you performed any audit to map data flows ?	Organisational question
			Does your application provide any information regarding the individual's rights ?	Right to be informed/Transparency
			The data being collected is sufficient to fulfill the consent purposes	Purpose
			Is your application only holding the data being used ?	Minimisation
			Is it possible to demonstrate your data minimization practices ?	Minimisation
			Is it possible to justify the time frame for the retained data ?	Retention period
			Does your application automatically deletes the data after the time frame expires ?	Retention period
			Does your application provides a way, so the individual can erease his data (right to erasure) ?	Forgotten
			Does your software record a users consent choices ?	Consent
			Is personal data being collected for the specified, explicit and legitimate purpose ?	Purpose
			Do the individuals have access to the purpose details ?	Purpose Right to be informed/Transparency
			Do you regularly update your purpose based on the changes made for the processing ?	Purpose
			Do you ask for new consent if the purpose changes ?	Consent
			Do you regularly review the data stored ?	Organisational question
			Can you still achieve your purpose, if the data collected is reduced ?	Minimisation
			Does you application provide mechanisms to keep data updated ?	Accuracy
			Do you inform individuals about their right of rectification ?	Right to be informed/Transparency
			Are you aware of your right to refuse requests for rectifications ?	Rectification
			Do you comply with the limit of one month to answer requests to update data (right of access) ?	Rights Access/rectification/...
			Does your application erase incorrect data ?	Accuracy
			Are you aware that you can keep data for longer then needed if you are only keeping it for public interest archiving, scientific or historical	Retention/ Purpose
			Do you have any mechanisms to anonymize data ?	Security
			Are you aware that the security of personal data is the date controller's responsibility ?	Security Organisational question
			Do you apply techniques to protect against unlawful and unauthorised processing ?	Security
			Do you have any measures regarding any data leak ?	Security
			Do you have any mechanisms to pseudonymize data ?	Security
			Does your application use encryption ?	Security
			Can you demonstrate compliance with the points answered before ?	Security Organisational question
			Do you clear data, when it is no longer needed ?	Accuracy
	Lawful basis and transparency		Conduct an information audit to determine what information you process and who has access to it.	Organisational question
			Have a legal justification for your data processing activities.	Record of processing activities
			Provide clear information about your data processing and legal justification in your privacy policy.	Right to be informed/Transparency
	Data security		Take data protection into account at all times, from the moment you begin developing a product to each time you process data.	Organisational question
			Encrypt, pseudonymize, or anonymize personal data wherever possible.	Security
			Create an internal security policy for your team members, and build awareness about data protection.	Security

[5]			Know when to conduct a data protection impact assessment, and have a process in place to carry it out.	DPIA
			Have a process in place to notify the authorities and your data subjects in the event of a data breach.	Breach
	Accountability and governance		Designate someone responsible for ensuring GDPR compliance across your organization.	DPO
			Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.	Third parties
			If your organization is outside the EU, appoint a representative within one of the EU member states.	Representative
			Appoint a Data Protection Officer (if necessary)	DPO
	Privacy rights		It's easy for your customers to request and receive all the information you have about them.	Access
			It's easy for your customers to correct or update inaccurate or incomplete information.	Rectification
			It's easy for your customers to request to have their personal data deleted.	Forgotten
			It's easy for your customers to ask you to stop processing their data.	Restriction
			It's easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.	Portability
			It's easy for your customers to object to you processing their data.	Objection
			If you make decisions about people based on automated processes, you have a procedure to protect their rights.	Automated Decision Making and Profiling/ rights
[3]	PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA	Article 6(1)	Is the legal basis for each processing activity documented ?	Legal basis
		Article 4(2)	Is the purpose for each processing activity documented ?	Purpose
		Article 4(1)	Will the personal data be processed for a purpose other than what was intended at the time of collection ?	Purpose
			Do consent-collecting mechanisms require some action (e.g., ticking a box) or affirmative statement by the data subject ?	Consent
		Article 9(1)	Where processing involving special categories of data is based on consent, is explicit consent obtained (e.g., in writing or verbally) from the data subject ?	Consent
	RIGHTS OF THE DATA SUBJECTS WHILE PROCESSING AND ACCESSING THEIR INFORMATION		Is a process in place to respond to requests for access to information held about a data subject ?	Access
			Is a process in place to rectify / delete information about a data subject pursuant to a request ?	Rectification Forgotten
			Is a process in place to communicate updates of personal data to third parties who have received the data ?	Third parties
		(According to Article 7(3) should be as easy fo	Is there a process in place to allow a data subject to revoke consent for a particular processing activity at any time ?	Withdrawal consent
			When consent for a particular processing activity is revoked, are there processes in place to ensure processing is stopped, including any processing by third parties ?	Withdral consent
			Is there a process in place to comply with requests to restrict the processing of data if requested by a data subject, including any processing by third parties ?	Restriction
			Is a process in place to comply with requests from a data subject to have their personal data transferred directly to another controller, if technically possible ?	Portability
			Is a process in place to stop processing for direct marketing purposes when an objection is received ?	Objection
		Article 4(4)	If engaged in automated decision making, including profiling, is there a process by which a data subject may request a manual review of the decision or profiling activity ?	Automated decision making and profiling.
		Article 27	Has a representative within the European Union been designated ?	Representative
	TRANSFERS OF DATA TO THIRD PARTIES		Do contracts with third parties specify that the third party, and any subcontractor that may be utilised, must have data protection and security protection clauses / annexes in place ?	Security Third parties
			Are records kept of all processing activities your company engages in ?	Record of processing activities
			Are all data transfers documented, including cross-border transfers ?	Transfers outside EU
			Is a data transfer mechanism in place in the event that personal data is to be transferred to a third country or international organisation ?	Transfers outside EU
	PRIVACY NOTICES		Is a Privacy Notice provided to data subjects no later than at the time information is collected from those data subjects ?	Right to be informed/Transparency
			Is a Privacy Notice provided to data subjects at every point of collection ?	Right to be informed/Transparency
			If data is to be processed for a secondary purpose, are data subjects notified of the new purpose prior to processing ?	Right to be informed/Transparency

			Does the Privacy Notice clearly specify how data subjects can exercise their rights under the GDPR ?	Right to be informed/Transparency
	DATA BREACHES		Is a process in place to ensure the appropriate Supervisory Authority is notified within 72 hours of a confirmed data breach ?	Breach
			Do agreements / contracts with third parties specify that the third party has to notify you (the controller) without undue delay after becoming aware of a data breach or potential data breach involving personal data ?	Breach Third parties
			Are internal policies in place defining what is considered to be a data breach and when and if notification to data subjects or Supervisory Authorities is required ?	Breach
		Article 33	Is a log kept of all data breaches that occur, along with the effects and remedial actions taken ?	Breach
		Article 24(1)	Are assessments of processing activities conducted by the relevant personnel to determine the data protection measures that should be in place, proportionate to the risks involved with the processing activity ?	Organisational question
			Is privacy assessed at the beginning stages of development of any processing activity ?	Organisational question
			Are measures such as data minimisation and pseudonymisation implemented across all applicable organisational units ?	Minimisation Security
	DATA PROTECTION IMPACT ASSESSMENT (DPIA)		Are Data Protection Impact Assessments (DPIAs) completed for processing activities involving special categories of information, automated decision making, or profiling ?	DPIA
			Are DPIAs completed prior to implementing new technologies, processes, or projects ?	DPIA

Transparency is included in the ""Right to be informed & Transparency"" criteria. In the GDPR, transparency is defined as:

"The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used."

We believe that this principle is closely linked to the right to information. It is the means by which the right to information is put into practice. This criterion is more concerned with the way in which information is information to users in order to ensure better understanding and effective communication regarding the collection, processing and use of their personal data, as well as their rights."

		Lawfulness				User rights									Accountability and Governance								Security & Breach		Transfer outside the EU.
		consent	consent and decisions for minors	legal basis	record of processing activities	To be informed	withdrawal of consent	access	portability	erasure	rectification	restriction	objection	automated decision making and profiling.	Purpose	accuracy	minimization	data retention,	third parties	DPO	DPIA	representative	Security	Breach.	Transfer outside the EU.
	[8]	✗	✗	✗		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		✗	✗	✗
	[1]	✗	✗	✗	✗	✗		✗	✗	✗	✗	✗	✗	✗		✗			✗	✗	✗		✗	✗	✗
	[38]	✗				✗		✗		✗	✗				✗	✗	✗	✗					✗		
	[5]				✗	✗		✗	✗	✗	✗	✗	✗	✗					✗	✗	✗	✗	✗	✗	
	[3]	✗		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗		✗		✗		✗	✗	✗	✗	✗