INTERNET SAFETY LABS

ISL Safe Software Specification
Websites and Mobile Apps
Data Controller Questionnaire

Version 1.1
RTS WG
06-Jun-22

VERSION	DATE	EDITORS	DESCRIPTION OF CHANGES
0.1	9/17/21	L. LeVasseur	Draft
1.0	6/6/22	L. LeVasseur	Changed name of organization and Me2B Marriage.

This workbook contains Data Controller Questionnaire.

DATA CONTROLLER QUESTIONNAIRE - WEBSITE OR APP

Note that this questionnaire assumes that the entity completing this information is the Data Controller.

		QUESTION	WHY WE ASK	RANGE OF ANSWERS	VENDOR RESPONSE
1		Name of URL or app to be tested.	To know what you want tested.	text;	
		INFORMATION SHARING PRACTICES			
2		Are you using the IAB's Transparency & Consent Framework?	Because the IAB's TCF has been found to be in breach of GDPR due to cross-company data sharing without the individual's permission. https://www.dataguidance.com/news/international-belgian-dpas-investigation-finds-iab-tcf	Yes / No	
3	A	Does this website or app USE information that has been OBTAINED from 3rd party data brokers? If yes, please explain: - What Data? - From what Data Broker or source? - How is data used in your business and in this product or website?	Gathering information via 3rd party data brokers may be disrespectful. Some uses are acceptable, such as: We advocate that any information about a person be collected/stored under a Me2B "Marriage" directly between the Me ("data subject") and the holder of the information (data broker in this case).	Yes - with explanation of how all the data is used in the business and product/ No	
	B	For each 3rd party vendor, what kind of privacy obligations are required (of you) as the recipient of the data?	Have you been passed the responsibilities of the original data collector?	Explanation.	
4	A	Does this website or app either directly or indirectly SELL or SHARE information with data brokers? If yes, please identify what data is sold/shared to/with whom, and for what purpose. Please also identify which Me2B Commitments trigger selling/sharing data with data brokers.	We are unable to measure back-end data sharing and transactions.	Yes - with explanation of how all the data is used in the business and product/ No	
	B	For each Data Broker receiving data from you, describe privacy requirements/obligations that you prescribe for the receiving entity. Do you require the receiving entity to pass that on to their receiving entitites?	To ensure data sharing rules are preserved to downstream recipients of data.		
5		Please identify all Data Processors used in this app. Include name of Company, product/service name, and a brief description of what purpose the Data Processor serves. Organize response by Me2B Commitment; i.e. list Data Processors per Me2B Commitment.	As a Data Controller, you are responsible for the Data Processors used in your service.	For each Me2B Commitment state: List of Company / Product or Service Name / Purpose, where Purpose can be: To Provide This Service (Me2B Deal) / To Subsidize the Cost of This Service / Marketing - Profile building? [what does this mean to me?] / Fraud Prevention / Personalized Experience? / Government or Regulatory Requirements / Social Good or Altruistic purposes	
6		Please identify the analytics platform/technology used in your website or app. Include details on data collection purposes, with particular attention on data aggregation practices, and specific settings that preserve Data Subject privacy.	Some analytics platforms share data with advertising platforms; this is an unsafe form of analytics. Additionally, analytics can be used to uniquely identify and/or profile Data Subjects, which is unlawful under GDPR and CPRA.	Name of Analytics platform, Description of collection practices and settings.	
		PERMISSION RECORDING PRACTICES			
7		Do you use a standardized structure such as the Consent Receipt v1.1 (https://kantarainitiative.org/download/7902) to record permissions? Please identify which commitments use the standardized structure, and if the records are available to the individual/Me.	Because Consent Receipt is a relatively new, state of the art practice to record/share/audit permissions and we can't detect use through observation of the website or app.	Yes / No for each Commitment	
For Questions 8-14, please respond if the website or app includes this type of commitment. If your website or app includes other commitments, please repeat question 14 as many times as you need for each additional commitment.					
		LOCATION COMMITMENT			

DATA CONTROLLER QUESTIONNAIRE - WEBSITE OR APP

Note that this questionnaire assumes that the entity completing this information is the Data Controller.

8	A	As the Data Controller, what happens when an individual disables location information sharing? Does the system remove the location history?	Disabling the "Location Commitment" should result in the location history being forgotten, including all downstream data processors, and location not being used or collected/correlated to the individual.	Description of system behavior.	
	B	How is location consent (granting and revocation) orchestrated with all of your Data Processors?	As a Data Controller, you are obligated to ensure consent enforcement throughout all Data Processors.	Description of how system automatically manages location consent between Data Controller and Data Processors.	
	C	How does your system ensure downstream Data Processors also remove location history when the individual disables location information sharing?	As a Data Controller, you are obligated to ensure consent management throughout all Data Processors	Description of the data deletion activity by Data Processors.	
	D	Please describe how long the system retains the location information. In your description please include any automatic purging logic (triggers). Also include if purge instructions automatically flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description of data retention practice/logic employed by the system.	
		CONTACT US COMMITMENT			
9	A	How is the user-entered data on the Contact Us form saved? In particular is it encrypted at rest and in transit?	To ensure that the data is protected.	Description of system behavior.	
	B	Is the user-entered data from the Contact Us form shared with Data Processors? Please identify which Data Processors, the purpose for sharing, and the limitations on Data Processor use and duration of saving.	To ensure that the data is shared only with Data Processors needed to provide the expected service, and that those Data Processors are bound with appropriate limitation on the use and saving of the data.	List of Data Processors who receive the Contact Us information, and the purpose for sharing with each. Description of the data use/sharing/storage limitations on the Data Processors imposed by the Data Controller.	
	C	Please describe how quickly the system deletes the Contact Us information. In your description please include any automatic purging logic (triggers). Also include if purge instructions automatically flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description of data retention practice/logic employed by the system.	
10	A	How is promotional communication status (enrolled/unenrolled) orchestrated with all of your Data Processors?	As a Data Controller, you are obligated to ensure consent management throughout all Data Processors	Description of how system automatically manages promotional communication status between Data Controller and Data Processors.	
	B	When an individual unenrolls from promotional communications, is all of their information completely removed from your files?	Unenrolling from the "Promotional Communications Commitment" should result all of the collected information (email, name, etc.) being forgotten, including all downstream data processors, and individual no longer receiving promotional communications.	Yes / No - explanation	
	C	When an individual unenrolls from promotional communications, is all of their information completely removed from downstream Data Processors' files?	Unenrolling from the "Promotional Communications Commitment" should result all of the collected information (email, name, etc.) being forgotten, including all downstream data processors, and individual no longer receiving promotional communications for Data Controller and all Data Processors.	Yes / No - explanation	
	D	When an individual is enrolled in promotional communication, do you create a profile for that individual associated with their email? If so, how do you use the profile? Do you share profile information with Data Processors?	Validating that profiling is used only for 1st party/vendor's use to personalize communications.	Yes + explanation / No	
	E	Please describe how long the system retains the promotional communication enrollment information. In your description please include any automatic purging logic (triggers). Also include if/how purge instructions flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description	

DATA CONTROLLER QUESTIONNAIRE - WEBSITE OR APP

Note that this questionnaire assumes that the entity completing this information is the Data Controller.

	F	When an individual is enrolled in promotional communications, do you share their email address with any 3rd parties? Please explain any sharing (who shared with/ what's shared/ for what purpose)	Validating that sharing of email information with 3rd parties is strictly to perform delivery of promotional communication.	Yes + explanation / No	
		LOYALTY PROGRAM COMMITMENT			
11	A	How is loyalty program status (enrolled/unenrolled) orchestrated with all of your Data Processors?	As a Data Controller, you are obligated to ensure consent management throughout all Data Processors	Description of how system automatically manages loyalty program status between Data Controller and Data Processors.	
	B	When an individual unenrolls from your loyalty program, is all of their information completely removed from your files?	Validating that an individual is forgotten when they unenroll from the loyalty program.	Yes / No - explanation	
	C	When an individual unenrolls from your loyalty program, is all of their information completely removed from all Data Processors' files?	Validating that an individual is forgotten when they unenroll from the loyalty program.	Yes / No - explanation	
	D	What information do you collect from someone when they are using your digital service and they are signed up in your loyalty program?	We compare your answer here to the observed product behavior for consistency.	Description, list	
	E	When an individual is enrolled in your loyalty program, do you share any of the gathered information with any 3rd parties? Please explain any sharing.	Validating that sharing of personal information with 3rd parties is strictly to perform delivery of the loyalty program.	Yes + explanation / No	
	F	Please describe how long the system retains the Loyalty program information. In your description please include any automatic purging logic (triggers). Also include if/how purge instructions flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description	
		ONE-OFF TRANSACTION COMMITMENT			
12	A	When an individual performs a one-off transaction [no personal account created], what information is shared with 3rd parties?	Validating that the sharing of personal information with 3d parties during a one-off transaction is strictly at the service of performing the transaction.	Description of information, who it's shared with and for what purpose.	
	B	Please describe how long the system retains the transaction information. In your description please include any automatic purging logic (triggers). Also include if/how purge instructions flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description	
		ACCOUNT CREATION ("Me2B Marriage") COMMITMENT			
13	A	What information is collected during the course of the Me2B relationship for registered users and how is it used?	Understanding the performance of data minimization.	Description of information and how it's used.	
	B	Is the information collected for registered users during the course of the Me2B relationship monetized to subsidize the price of the service?	Validating if data monetization is occuring	Yes + explanation / No	
	C	Is the information collected for registered users during the course of the Me2B relationship shared with 3rd parties (including account credentials]? With whom and for what purpose?	Validating if 3rd party sharing of personal information is strictly done to deliver the service to the individual.	Description of information that's shared, who it's shared with and for what purpose.	
	D	How is account creation status orchestrated with all of your Data Processors?	As a Data Controller, you are obligated to ensure consent management throughout all Data Processors	Description of how system automatically manages loyalty program status between Data Controller and Data Processors.	
	E	When an individual deletes their account, is all of their information deleted and are they forgotten? If not, how does the individual request their information be deleted?	Validating if the individual is reasonably forgotten when ending the Me2B Relationship.	Description of what happens when the individual stops service, and if/how they can request that their information be deleted. What information can/can't be deleted?	
	F	When an individual requests that their account be closed, is all of their information completely removed from all Data Processors' files?	Validating that an individual is forgotten when they close their account.	Yes / No - explanation	
	G	Please describe how long the system retains account information. In your description please include any automatic purging logic (triggers). Also include if/how purge instructions flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description	
		OTHER COMMITMENT(s)			
14	A	How is this commitment (enrolled/unenrolled) orchestrated with all of your Data Processors?	As a Data Controller, you are obligated to ensure consent management throughout all Data Processors	Description of how system automatically manages commitment status between Data Controller and Data Processors.	

DATA CONTROLLER QUESTIONNAIRE - WEBSITE OR APP

Note that this questionnaire assumes that the entity completing this information is the Data Controller.

	B	When an individual unenrolls from this commitmnet, is all of their related information completely removed from your files?	Validating that an individual is forgotten when they unenroll from the commitment.	Yes / No - explanation	
	C	When an individual unenrolls from this commitment, is all of their information completely removed from all Data Processors' files?	Validating that an individual is forgotten when they unenroll from this commitment.	Yes / No - explanation	
	D	What information do you collect from someone when they are using your digital service and they are enrolled in this commitment?	We compare your answer here to the observed product behavior for consistency.	Description, list	
	E	When an individual is enrolled in this commitment, do you share any of the gathered information with any 3rd parties? Please explain any sharing.	Validating that sharing of personal information with 3rd parties is strictly to perform delivery of this commitment.	Yes + explanation / No	
	F	Please describe how long the system retains the commitment-related information. In your description please include any automatic purging logic (triggers). Also include if/how purge instructions flow to Data Processors.	It's difficult for us to readily measure data retention practices, thus we request a description of the system specifications relating to data retention and purging.	Description	
		3RD PARTY VENDOR (DATA PROCESSOR) MANAGEMENT PRACTICES			
13	A	Have you created special data pipelines for particular partners [that have not already been described in this questionnaire]? Please list the name of each partner, the nature of the pipeline, including what data is being shared and for what purpose.	To ensure that all possible data sharing is addressed in this audit.	Description	
	B	Have you received information from all of your vendors about their privacy practices, and have you integrated that into your Privacy Policy and Terms of Service? Please provide a list of all the data controllers from whom you've received detailed privacy practices.	To validate that your legal policies are reflective of all data processor practices.	Description and List of data processors.	
	C	Do you include privacy requirements in your SLAs with Data Processors? If so, please provide an example.	To ensure that your data handling requirements are provided to data processors.	Description	
	D	[For apps] Please complete requested information on SDK Tab in the SDK Audit tab of the App Raw Data workbook.	Used to validate data sharing with SDKs.	See SDK Audit Tab in the App Raw Data workbook.	
	E	[For apps] Please complete requested information on app Permissions Audit tab of the App Raw Data Workbook.	Used to validate data collection.	See App Permissions Audit Tab in the App Raw Data workbook.	
		INFORMATION SECURITY PRACTICES			
14	A	Do you provide security source code reviews for products (web-based or mobile) source code under development or enhancements - Static Application Security Testing (SAST)?	To exhibit that security is being applied during the software development lifecycle (SDLC) https://www.gartner.com/en/information-technology/glossary/static-application-security-testing-sast	Description	
	B	Do you provide runtime security reviews for products (web-based or mobile) prior to in production status - Dynamic Application Security Testing (DAST)?	To exhibit that security controls applied in development are in place and operable before applications as pushed to production. https://www.gartner.com/en/information-technology/glossary/dynamic-application-security-testing-dast	Description	

DATA CONTROLLER QUESTIONNAIRE - WEBSITE OR APP

Note that this questionnaire assumes that the entity completing this information is the Data Controller.

	C	Do you conduct Manual Penetration Test (Pen-Test) to assess security controls and application logic for products (web-based or mobile) prior to in production status or in production - Manual Penetration Test (MPT)?	To exhibit that security controls applied in development and tested in runtime Dev/QA/Staging environments are validated; to include data protection, encryption, and identity and access management protocols https://www.gartner.com/en/information-technology/glossary/penetration-testing	Description	
	D	Do you conduct vulnerability management assessments to continually assess infrastructure security controls (i.e. servers, network, etc.) and application security controls (web-based or mobile) to detect and respond to misconfiguration, security patches, zero-day vulnerabilities, etc?	To exhibit that Continuous Monitoring (ConMon) is active and responsive to manage security controls and vulnerabilities within product(s) and across the IT enterprise https://www.gartner.com/en/information-technology/glossary/vulnerability-assessment	Description	
	E	Describe your data encryption practices, including at rest and in transport.	To ensure the highest level of data encryption practices.	Description	