CHDI Foundation, Inc. – Data Security Questionnaire

Question:	Introduction and explanation for collection of this information: To comply with GDPR, CHDI is required to obtain information regarding the planned use/processing, hosting and storage of data and the data security and protection measures to include information on applicable data security policies for this organization.	Instructions:	Answer:
1	What is the full legal name of the organization that will receive the data?	(NOTE: The organization receiving the data must be the same as the organization that will sign the agreement pursuant to which the data will be provided to such organization)	
2	What country is this organization established in?	(NOTE: The organization receiving the data must be the same as the organization that will sign the agreement pursuant to which the data will be provided to such organization)	Name of Country: [_____]
3	If this organization is established in a European Union (EU) country, please provide the name of Data Protection Commission/Office the Organization is subject to (and, as applicable, the Organization's registration number)	EU Country list as of August 30, 2021 (reference): (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden)	Name of Data Protection Commission/Office the Recipient is Subject to (and, as applicable, the Organization's registration number): [_____]

4	If this organization is not established in an EU country, does the country this organization is established (or, alternatively, does the organization itself) hold a European Commission Decision that such country (or, alternatively, organization) provides an adequate level of protection in accordance with Article 45 of the GDPR? If YES, provide details.	Provide Details and Information of the Applicable Finding of the European Commission Related to Adequate Level of Protection in Accordance with Article 45 of the GDPR: Non-EU Country list that hold a European Commission Decision as of February 27, 2022: (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en): The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.	Provide Details and Information of the Applicable Finding of the European Commission Related to Adequate Level of Protection in Accordance with Article 45 of the GDPR: [_____]
5	Has this organization appointed a Data Protection Officer? (YES/NO)	If Q5 = YES, go to Q6. If Q5 = NO, go to Q7.	
6	If Q5 = YES, Provide the contact details of this organization's Data Protection Officer(s)?		Data Protection Officer Name: Address: Position: Email: Phone:
7	If Q5 = NO, Provide the contact details for this organization of the person responsible for data protection matters.		Person Responsible for Data Protection Matters Name: Address: Position: Email: Phone:

8	Is this organization planning on transferring the data to any third-party recipient in any of the following categories? 1. Any affiliate (YES/NO) 2. Any fee for service providers (e.g., CROs) (YES/NO) 3. Any other third-party (YES/NO) 4. Any third-party hosting providers (e.g., AWS) or managed services providers (YES/NO)	Please provide the following for each of the third-party recipients:	Full legal name of each third-party recipient: Type of third-party recipient (i.e., affiliate; fee for service provider; other third-party; third-party hosting providers) Individuals' Name: Address: Phone: Facsimile: Email: Country: The purpose for the transfer and use by such third-party recipient:
9	Have (or will) all listed third-party recipients where the data is planned to be used/processed, hosted or stored sign an agreement covering such use/processing, hosting and storage of the data?		
Order	**DATA USE INFORMATION** **Please complete the following data security questionnaire. If this organization already has a Technical and Operational Measures (TOMs) document, please upload that as well. You may find it easier to provide links to this organization's SOPs, and/or provide the organizations security SOPs. This is also acceptable given that these documents cover the below security items.**		
1	List all countries where the data will be used/processed, hosted or stored?		Name of Country (Countries): [_____]
2	Does this organization hold an ISO 27001 certification? (i.e., Is this organization ISO certified?) (YES/NO)	If Q2 = NO, go to Q3	
3	If Q2 = NO, Does this organization hold any industry recognized security certification(s) from any accredited third party? (YES/NO)	If Q3 = YES, please list all security certifications.	

4	What technical and organizational security measures (TOMs) does this organization employ that will protect the data provided by CHDI in this organization's computer systems, operating systems, network, applications and databases?	For example: encryption, password protections, mandatory logins, testing, ability to restore availability and access to data in the event of a physical/technical event, segregation of data, access control systems, card readers for access to areas, back-ups, confidentiality agreements, system updates and patching If possible, please provide an electronic copy of this organization's technical and organizational security measures (TOMs) in either pdf/docx format or via a HTML link.	
5	Please describe this organization's detailed data access and control policy?	For example: authorization, management, implantation processes. Include: Bring Your Own Device (BYOD) policies if applicable, unauthorized device (flash drives, tablets, external drives, etc.) policies and data access logging policies.	
6	Please describe this organization's data encryption policy (in transit and at rest)?		
7	Has this organization had a security assessment performed (Penetration (PEN) test, vulnerability scan, etc.)? (YES/NO)	If Q7 = YES, please provide date performed and any related findings.	
8	Has this organization experienced a security breach resulting in a loss or unauthorized disclosure of personal data within the past six years? (YES/NO)	If Q8 = YES, provide details of each incident and how it was resolved.	
9	Please describe this organization's data breach reporting, notification, tracking and resolution policy?		
10	Please describe this organization's data security risk mitigation policy?		
11	Please describe this organization's audit process for maintaining compliance for information and data security?		
12	Please describe this organization's data and records retention policy?		

13	Does this organization have a business continuity and disaster recovery plan? (YES/NO)	If Q13 = YES, please provide details on the business continuity and disaster recovery plan.	
14	Are this organization's security and privacy policies reviewed and updated periodically? (YES/NO)	If Q14 = YES, please provide details on how often it is reviewed and updated.	
15	Does this organization routinely perform training on the handling of personal data and information security? (YES/NO)	If Q15 = YES, please provide details describing the type of training and the frequency.	
16	Please provide an electronic copy of any other organization policy(ies) (in pdf/docx format or via HTML link) which this organization would like to provide in response to any of the above questions.		