Partner / Vendor Request for Information – Privacy, Data Protection and Security

|  |  |  |
| --- | --- | --- |
| **Third Party Contact Information** |  | Suggested responses |
| 1 | Company name: | [Company Name] |
| 2 | Location of Head Office: | [Company Address] |
| 3 | Account manager / Contact name: | [Account Manager / Contact Name, where applicable] |
| 4 | Account manager / Contact phone number: | [Contact Phone Number] |
| 5 | Account manager email address: | [Contact email address] |
| 6 | Please describe the nature of the business relationship and activities | [summary of contract type (where applicable), scope, DP relationship (Controller to Controller, Joint Controller, Processor, Sub-processor) |
| **Data Protection Representative** | |  |
| 7 | Data Protection Contact name: | [DP lead name] |
| 8 | Data Protection Contact email address: | [DP lead email address] |
| 9 | Data Protection Contact phone number: | [DP lead phone number] |
| **Certifications and Standards** |  |  |
| 10 | ISO 27001 Information Security | [status – uncertified / certified (if certified, provide link to evidence) |
| 11 | ISO 9001 Quality Management | [status – uncertified / certified (if certified, provide link to evidence) |
| 12 | ISO 22301 Business Continuity | [status – uncertified / certified (if certified, provide link to evidence) |
| 13 | ISO 20001 Service Management | [status – uncertified / certified (if certified, provide link to evidence) |
| 14 | PCI DSS | [status – uncertified / certified (if certified, provide link to evidence) |
|  | Cyber Essentials/Cyber Essentials Plus | [status – uncertified / certified (if certified, provide link to evidence) |
| **Data Protection Compliance (DPA\GDPR)** |  |  |
| 15 | Does your organisation operate in full compliance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA)? Including the following principles: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Security • Accountability | [Please provide links to relevant privacy policies, security policies and/or references to sections within data processing agreements / data sharing agreements – please be aware that specific questions below may ask for more detail and should refer to that section] |
|  | Do you consider your provision of services to fall within the scope of the Age Appropriate Design Code? If so, can you confirm that you are compliant with the requirements of the Code, and provide any evidence of certification. | [the code is available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/> and applies to Information Society Services that are aimed at, or likely to be accessed by, children] |
| 16 | What customer data do you process, store or transmit? (if any) e.g. documents, staff details, customer names, addresses, account numbers, PAN data, audit reports, system backups, contracts, service management records, source code, multimedia. | [details of all data elements, data categories and any other relevant information. Please note that this is asking what data is processed, not just what Personal Data is processed] |
| 17 | Are you registered with the UK Information Commissioners Office (or equivalent)? If so, please provide details (registration number) |  |
| 18 | How is data transmitted to\from customers? Please detail the methods, volumes and frequencies | [This may also be covered in sections below, but please provide a summary] |
| 19 | At what locations is customer data stored, transmitted or processed? Please also detail any Third Country transfers. | [please note that this is for locations outside of UK, and references to any adequacy agreement, SCCs and additional measures that may be relevant. Please refer to sections 23-25 below, if applicable] |
| 20 | Do you maintain 'Records of Processing' (GDPR Article 30), detailing at least the purpose of processing, categories of data subjects, categories of personal data, data retention and data sharing activities? | [please remember that this is in reference to the data that is being shared with your relevant to this service, not for B2B as your customer. Please refer to the DPA or DSA as needed] |
| 21 | Please describe your Data Retention Schedule and capabilities as it relates to customer Personal Information | [please remember that this is in reference to the data that is being shared with your relevant to this service, not for B2B as your customer. Please refer to the DPA or DSA as needed] |
| 22 | Approximately how many people have access (or could obtain access) to customer data? (excluding customer employees) | [please ensure that you include details from relevant sub-processors, where applicable, as well as your own staff. Where data is shared with third parties (other controllers) due to the use of the service, please ensure all details are in sections 23 and 24 below] |
| **External Parties** |  |  |
| 23 | Is data shared with, or processed by, any third parties or sub-processors? If so, please provide details. | [Please ensure that you separate third parties (other controllers that may be using the data for their own purpose) and sub-processors (where the same instructions from the controller operate)] |
| 24 | If shared with third parties, how is compliance with data protection obligations and the security of data maintained? | [please provide references to the relevant evidence] |
| 25 | Are processing agreements and NDAs in place with all sub-processors or third parties that may have access to sensitive information and\or intellectual property? | [please provide references to the relevant evidence] |
| **Policies, Processes and Procedures** |  |  |
| 26 | Does the organisation operate any Security Policies? Eg Information Security Policy, Acceptable Use Policy. If so, please list or describe. | [please provide references to the relevant evidence] |
| 27 | Does the organisation have documented agreement and commitment to information security from top management? | [please provide references to the relevant evidence] |
| 28 | Is there a mechanism established to ensure employees have read and agreed to security policies applicable to them? | [please provide references to the relevant evidence] |
| **HR Controls** |  |  |
| 29 | Are all employees subject to security awareness training? At what point and frequency are employees provided with such training? | [please provide references to the relevant evidence] |
| 30 | Has the organisation appointed one or more resources to be responsible for information security? If so, please provide roles and responsibilities. | [please provide references to the relevant evidence] |
| 31 | Are new employees subject to background checks prior to employment? If so, please detail what checks are undertaken. E.g. CRB\DBS | [please provide references to the relevant evidence] |
| **Risk Management** |  |  |
| 32 | Is a risk assessment conducted at a frequency no less than once per year? | [please provide references to the relevant evidence] |
| 33 | Are individual information security risks recorded using a risk register? | [please provide references to the relevant evidence] |
| 34 | Are identified risks measured, prioritised and remediated using a risk treatment plan? | [please provide references to the relevant evidence] |
| **Incident Management** |  |  |
| 35 | Have you had any security incidents within the last year? (e.g. crime, fraud, attempted fraud, breach of security policy, system intrusion). If so, please provide reports and supporting information. |  |
| 36 | Do you have a notification process whereby customers and clients will be made aware of any relevant incidents? (Including Data Protection Breaches) | [please provide references to the relevant evidence] |
| 37 | Do you have an established and documented methodology for identifying and responding to security incidents? | [please provide references to the relevant evidence] |
| **Physical Security** |  |  |
| 38 | Please detail physical security controls regarding access to facilities. For example: access cards, turnstiles, CCTV, intruder alarms | [please provide references to the relevant evidence] |
| 39 | Are any sensitive areas subject to additional security or availability controls? If so, please provide details on such controls. | [please provide references to the relevant evidence] |
| 40 | Do you have a method of identifying visitors, and recording visitor history to physical premises? Please describe. | [please provide references to the relevant evidence] |
| **Network Security** |  |  |
| 41 | Do you have accurate and maintained network diagrams and documentation detailing endpoints, egress points and traffic flows? | [please provide references to the relevant evidence] |
| 42 | Are penetration testing exercises conducted at least every 6-12 months? If so, please provide details (provider, tools, scope). | [please provide references to the relevant evidence] |
| 43 | Are controls in place to monitor and control internet and email access? E.g. spam filters and content filters. Please provide details. | [please provide references to the relevant evidence] |
| 44 | Are centrally managed Anti-Virus and Anti-Malware controls deployed within the infrastructure? If so, please provide details. | [please provide references to the relevant evidence] |
| 45 | Is there an established and practiced patching strategy in place? If so, please provide details. | [please provide references to the relevant evidence] |
| 46 | Do you have a method of identifying network security vulnerabilities? If so, please provide details. | [please provide references to the relevant evidence] |
| 47 | Is there an appropriate logging system in place to collect system and event logs from across the estate? Please provide details. | [please provide references to the relevant evidence] |
| **Data Encryption** |  |  |
| 48 | If customer data traverses public or unprotected networks, is it protected by a strong encryption algorithm? If so, what encryption is used? | [please provide references to the relevant evidence] |
| 49 | Is customer data encrypted at rest? (Servers, Databases, Backus etc) If so, what encryption algorithms are in use? | [please provide references to the relevant evidence] |
| 50 | Through what interfaces does the organisation transfer business data? How are these adequately secured? | [please provide references to the relevant evidence] |
| 51 | Are employee laptops encrypted? If so, please describe these controls. | [please provide references to the relevant evidence] |
| **Access Control** |  |  |
| 52 | Are access levels granted according to principle of least privilege? | [please provide references to the relevant evidence] |
| 53 | Are access levels reviewed on a regular basis? If so, at what frequency? | [please provide references to the relevant evidence] |
| 54 | Are user accounts attributable to uniquely identifiable individuals to ensure accountability and nondisruptive revocation of access? i.e. no shared accounts. Please detail any exceptions + compensating controls | [please provide references to the relevant evidence] |
| 55 | Are password criteria for networks, operating systems and applications sufficiently complex? (Please describe) | [please provide references to the relevant evidence] |
| **Business Continuity** |  |  |
| 56 | Do you have a business continuity plan? If so, please provide details and supporting evidence. | [please provide references to the relevant evidence] |
| 57 | Are business continuity and disaster recovery plans tested on a regular basis? If so, please provide details and supporting evidence. | [please provide references to the relevant evidence] |
| 58 | Are backup and restore procedures tested on a regular basis? At what frequency, and to what extent does this occur? | [please provide references to the relevant evidence] |
| 59 | What is the recovery point objective and recovery time objective for disaster recovery? (if available) | [please provide references to the relevant evidence] |
| **Software Development (if applicable)** |  |  |
| 60 | Are development processes and practices defined and documented, including security consideration and best practices? | [please provide references to the relevant evidence] |
| 61 | Are software developers trained in secure coding methods and practices? If so, please provide details. | [please provide references to the relevant evidence] |
| 62 | Are internally developed applications (including web applications) subject to penetration testing at least once per year? | [please provide references to the relevant evidence] |
| 63 | Are development and testing environments adequately separated from live\production environments and data? Please provide details. | [please provide references to the relevant evidence] |
| 64 | Where applicable, does your product support Single-Sign-On (eg SAML) to integrate with customer systems user credentials. | [please provide references to the relevant evidence] |

We appreciate you time in responding to this Request for Information.

Completed by ………………………………………………………………………..

Position ………………………………………………………………………..

Date ……………………………………………………………………….

# Acknowledgements

This template is prepared by Tony Sheppard - My Data Protection World.

Original design and contribution by Elliott [name] – ParentPay as part of the Education Data Matters group (<https://www.educationdatamatters.org.uk>).

Additional contributions by Alexander Banthien (GDPRiS), Claire Archibald (Education Data Hub, Derbyshire County Council) and Jessica Sweet (Coventry City Council).

Peer review and contributions by the DPOaaS Slack Group Community.

This is version 1.1 – 3rd September 2021.

This template is released under Creative Commons licence as part of Open Source projects from My Data Protection World. Please visit <https://www.mydataprotection.world> for more information.

Partner / Vendor Request for Information – Privacy, Data Protection and Security © 2021 by Tony Sheppard is licensed under Attribution 4.0 International. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>