|  |  |  |  |
| --- | --- | --- | --- |
| Vendor Name |  | | |
| Vendor Contact’s Name |  | Vendor Contact’s Phone Number | Product |
| Vendor Contact’s Email |  | Date Completed |  |

|  | **Inquiry** | **Select All that Apply** | **Additional Information** |
| --- | --- | --- | --- |
| 1 | Are you planning to comply with the General Data Protection Regulation (GDPR) by 5/25/2018? | Yes  No | If No, explain why?  Click or tap here to enter text. |
| 2 | What GDPR requirements will you have completed by 5/25/18? | ☐ GDPR Compliant Privacy Notice (GDPR Articles 13, 14)  ☐ Controller/Processor Data Protection Addendum (GDPR Articles 28-32) (If complete, please provide to LUC; if incomplete, LUC will provide)  ☐ Record of Processing (GDPR Article 30) (including data mapping)  Consent to Process Special Categories of Personal Data (Article 9) (if required)  Consent to Process Special Categories of Personal Data (Article 9) (if required)  Consent to Process Using Automated, Individual Decision-Making, Including Profiling (Article 22) (if required)  Consent to Transfer Data to Third Country (Article 49) (if required)  Ability to respond to data subject requests and directions (Articles 15-22)  Are you a Privacy Shield Framework member?  Other | If selected other, please describe:  Click or tap here to enter text. |
| 3 | What is your data retention policy as it pertains to your LUC data that you process ("Loyola Data") | Less than 1 year  Between 1-3  Greater than 3 years  Customer driven  Term of the Agreement  None | If None, explain why?  Click or tap here to enter text. |
| 4 | Where is the location of processed/stored/collected Loyola data? | United States  European Union  All other geographic locations outside of the EU and US | If selected “All other geo locations”, which countries or continents is the data stored in currently?  Click or tap here to enter text. |
| 5 | Is Loyola data sent to other sub-processors for further processing? | Yes  No | If answer to 5 is a “Yes”, then answer 5a-5c, else skip them. |
| 5a | Have you entered into contracts with sub-processors who sub-process Loyola Data? | Yes  No  Not Applicable | If the answer to 5a is “No” or “Not Applicable” then explain why?  Click or tap here to enter text. |
| 5b | Where is the location of sub-processed/stored/collected Loyola data? | United States  European Union  All other geographic locations outside of the EU and US | If selected “All other geo locations”, which countries or continents is the data stored in currently?  Click or tap here to enter text. |
| 5c | Have you executed a GDPR Data Protection Addendum with each sub-processor? | Yes  No  Not Applicable | If the answer to 5c is “No” or “Not Applicable” then explain why?  Click or tap here to enter text. |
| 6 | Do any third-parties have access to our customer's data? For example:  Do you share our data for research or marketing purpose? | Yes  No | If the answer to “6” is a “Yes”, please answer 6a, else skip |
| 6a | Where is the location processed/stored/collected Loyola data? | United States  European Union  All other geographic locations outside of the EU and US | If selected “All other geo locations”, which countries or continents is the data stored currently?  Click or tap here to enter text. |
| 7 | Do you have or will you be appointing a Data Protection Officer (DPO)? | Yes  No |  |
| 8 | Have you appointed a GDPR Representative in the EU? | Yes  No | If selected “Yes”, where in the EU are they appointed?  Click or tap here to enter text. |
| 9 | Have you had a data breach in last 5 years? | Yes  No |  |
| 10 | Will you report any data breaches to us within 24-48 hours so we can comply with the 72 hours breach notification requirement set by GDPR for data breach? | Yes  No |  |
| 11 | Does your company have other legally mandated requirements for protecting data? Select all that apply. | HIPAA  GLBA  PCI  Other  None | If selected “Other”, please list them:  Click or tap here to enter text. |
| 12 | Do you train your staff regularly on data protection? | Yes  No | If yes, how often?  Semi-Annually  Annually  Ad-hoc |
| **Security** | | | |
| 13 | What types of Access Controls (authentication, authorization) do you have in place to prevent unauthorized users to reach your customers’ data? | Multi-factor authentication  Strong password protection  Least privilege  SSH  Other | If selected “Other”, please describe:  Click or tap here to enter text. |
| 14 | Does your team have access to our data? | Yes, unlimited  Yes, with consent  No |  |
| 15 | What methods are used for data protection? | Encryption In Motion  Encryption at Rest  Pseudonymization/Masking  Data Loss Prevention (DLP)  Other: | If selected “Other”, please describe:  Click or tap here to enter text. |
| 16 | Where can our data be potentially stored/travel in clear? | Inside your network perimeter  Outside your network perimeter  Secondary databases (backup db, non- prod db, data warehouse)  Nowhere you are aware of |  |
| 17 | Do you have an incident management and response process? | Yes  No |  |
| 18 | What type of secure software development processes do you have in place? Select all that apply. | Threat Modeling  Static/Dynamic Analysis  Pen Testing  Other: | If selected “Other”, please describe:  Click or tap here to enter text. |
| 19 | What steps do you take to address these vulnerabilities in your systems? | Apply patches  System upgrades  Other: | If selected “Other”, please describe:  Click or tap here to enter text. |
| 20 | Do you have an internal program for social engineering user awareness? | Yes  No |  |
| 21 | What 3rd party assessments of your security controls are in place? | SOC2 Type 1/2  External Audits  Internal Audits  Other: | If selected “Other”, please list them:  Click or tap here to enter text. |
| Additional Comments | | | |
| 28 | Click or tap here to enter text. | | |