MIT Computational Law Report •

Model DPA for Government for the Development of Exposure Alerting Applications and Systems

Cari Spivack, Colleen Brown, Dean Forbes, Michael R. Roberts

Published on: May 20, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

Background

U.S. Digital Response connects governments with experienced, pro bono technologists to provide rapid, effective response to the COVID-19 crisis. We are a volunteer-run and non-partisan team. As government leaders determine what role exposure alerting apps will play in opening society back up, we considered how our government partners can protect privacy and build trust with the public so these apps could achieve the high adoption rate necessary to make them effective.

One way to build trust is with a data governance program that prioritizes privacy, security and transparency. We drafted this model Data Protection Agreement to provide government and app developers with a data protection accountability mechanism that safeguards the privacy of individuals' data and encourages transparency at every stage of an app's development and deployment.

If you want to know more or get help using the DPA email dpa@usdigitalresponse.org

---

Introduction

This document provides guidance for creating an agreement for privacy and security standards related to the development of an exposure alerting software solution ("Software"). While the law provides a backdrop for the protection of and requirements for the processing of personal data as well as data that constitute government records, it does not necessarily answer the question of how commercial relations and data rights must be structured in all possible Software deployments. To foster the necessary trust in Software that will lead to popular use, and thus make Software effective for public health objectives, U.S. Digital Response encourages the implementation of data protection accountability mechanisms for both public and private entities. This model data protection agreement ("DPA") helps provide such accountability, and so U.S. Digital Response makes this DPA publicly available.

This model DPA considers existing data protection laws and regulations as a baseline and prescribes a framework with a high standard of data governance, and by providing this as a proposed contractual agreement, it creates an enforceable mechanism for additional accountability. The DPA also assimilates considerations from Privacy By Design, Fair Information Principle Practices, thought leadership from a variety of interested stakeholders including privacy, security and civil liberty organizations, government agencies, industry and technology companies and associations, as well as

public health professionals, including the CDC and epidemiologists. However, it is important to note that information and guidance pertaining to the COVID-19 pandemic changes on a daily – if not hourly – basis and may become stale very quickly. Parties are thus encouraged to consider the most updated regulatory and public health guidance as appropriate. In addition, this DPA is designed as a starting point to flexibly cover a broad range of potential data governance scenarios. Particular circumstances—including the technology requirements—may differ. We suggest the parties tailor the DPA to address particular circumstances with the advice of legal counsel.

These model provisions do not constitute legal advice, and are not intended to be used as a replacement for advice of counsel.

Data Protection Agreement

THIS DATA PROTECTION AGREEMENT (this "**DPA**") is effective as of this ____ day of _____, 202_ by and between **_____** (the "**Client**"[1]) and _____ (the "**Consultant**"), together the "**Parties**".

WHEREAS, the Client desires to develop an application for public health risk analysis and reporting ("Software") that will collect user data relating to public health imperatives, including the containment of COVID-19;

WHEREAS, the Client and the Consultant desire to execute this DPA to provide an accountability mechanism to foster the trust necessary for popular use of the Software;

NOW, THEREFORE, the parties agree to the following data protection provisions:

1. Definitions[2]

For purposes of the DPA the following definitions apply

"**Client Data"** means all data submitted to the Client for purposes of the Objective. Client Data may include Personal Data and Deidentified Data that the User has consented to provide to Client pursuant to the terms of the applicable privacy policy.

"**Consultant Data**" means data relating to the operation, performance, support and/or use of the Software. Consultant Data may include any Personal Data that the User has not consented to provide to Client pursuant to the terms of the applicable privacy policy, but which must be collected for the operation of the Software.

"**Data Protection Law**" means all laws, regulations, and regulatory guidelines issued by a government entity in any jurisdiction in which the Software is provided or received or which are otherwise applicable to the operation of the application relevant to the collection, processing, use, disclosure, safeguarding, retention or destruction of Personal Data.

"**Data Security Incident**" means any identified or reasonably suspected unauthorized or unlawful processing of, disclosure of, or access to, Personal Data and/or any accidental or unlawful destruction of, loss of, alteration to, or corruption to Personal Data.

"**Deidentified Data**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer and that has been protected by (i) technical safeguards that prohibit reidentification of a natural person; (ii) business processes that specifically prohibit reidentification of the information; (iii) business processes that prevent inadvertent release of deidentified information. The method of creating Deidentified Data shall be made publicly available and shall comply with data deidentification best practices, for example the HIPAA standard.

"**Personal Data**" means any personal data that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular User or any other natural person, or any other personally identifiable information as defined in an applicable Data Protection Law processed by either party hereto under or in connection with this DPA.

"**Processing"** means any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Software"** means computer software (including websites, HTML code, firmware and other software embedded in hardware devices), programs, data files, source and object codes, APIs, tools, user interfaces, algorithms, manuals, models and methodologies, and other specifications and documentation and all know-how relating thereto for the purposes of exposure alerting software solution.

"**User"** means any natural person that uses the Software, or otherwise is considered a consumer or data subject under applicable Data Protection Law.

"**Secondary Use**" is any use of Personal Data collected from the Software that is not aligned with the context in which it was collected, the Purpose(s) and the Objective(s) that were disclosed to the User at the time of collection.

2. Data Protection Requirements

2.1 Purpose[3]

The parties will define each Purpose(s) to address a specific public health need that the Software intends to solve, and restrict use of the Software for any other Purpose(s). For the avoidance of doubt, purposes that are not permitted include, but are not limited to, the following: law enforcement, immigration enforcement, tax collection, or commercial marketing.

2.2 Objective

The parties will define the Objective(s) of the Software specifically and narrowly. An Objective(s) shall:

2.2.1 Define the scope the Software's Purpose into individual and actionable goals;

2.2.2 Provide a clear explanation of how Software will achieve the Objective;

2.2.3 Establish criteria for measuring Software success in achieving the Objective(s).

2.3 Purpose Limitation

The collection, use, and retention of Personal Data must be fair, lawful and limited to that which is necessary to achieve an Objective.

2.3.1 Personal Data shall be Processed only for identifying, responding to, and addressing public health risks as identified in an Objective.

2.3.2 Personal Data shall not be used for a Secondary Purpose without the separate, prior express, informed and opt-in consent of the individual whom the Personal Data relates.

2.3.3 Use of the Software may not be conditioned on the acceptance of a Secondary Purpose.

2.4 Data Minimization

The collection and Processing of Personal Data should be kept to the minimum necessary to achieve an Objective.

2.4.1 The default should begin with non-identifiable interactions and transactions. Deidentified Data will be used to the greatest extent possible to achieve an Objective.

2.4.2 Wherever possible, identifiability and linkability of Personal Data should be minimized.

2.4.3 Parties shall take steps to prevent the reidentification of deidentified data.

2.5 Collection, Use, Retention, and Disclosure Limitation

The collection, use, retention, and disclosure of Personal Data shall be limited to the specific purposes disclosed to the User and for which User has provided opt-in consent, except where otherwise required or explicitly provided for by law.

2.5.1 Personal Data shall be retained only as long as necessary to fulfill Objective(s) and stated Purpose(s), and then securely destroyed.

2.5.2 The parties intend for Personal Data collected by Software to be destroyed when Software either achieves its Objective(s) or Software is unable to achieve Objective(s).

2.5.3 Where the need or use of Personal Data is not clear, there shall be a presumption of privacy and the default settings shall be the most privacy protective.

2.5.4 Software shall be designed to prevent the observability of exposure alert communications to other Users other than those expressly authorized by the User.

2.5.5 Software shall be designed to maximize use of anonymization, pseudonymization, encryption, decentralization and localized device-level data processing technologies.

2.5.6 Software shall not collect or otherwise Process the Personal Data of children without the verified, prior express consent of their parent or guardian in compliance with applicable Data Protection Laws.

2.6 Transparency

Client shall be transparent about Purpose(s), Objective(s), the Software’s effectiveness in achieving Objective(s), the Client’s data practices, and the legal framework and

authorities upon which the Client operates the Software.

2.6.1 Consultant, with assistance from Client, as appropriate, shall provide users with a clear and conspicuous privacy policy in the Software that uses plain language to inform Users about what Personal Data is collected from them, the sources of Personal Data, the purposes of the use of their Personal Data, what parties and for what purposes their Personal Data is shared, how long their Personal Data is maintained, their data privacy rights, and how the Client ensures Personal Data is protected. When applicable, the privacy notice should also disclose the creation, use and disclosure of Deidentified Data.

2.6.2 Client and Consultant shall issue weekly transparency reports that are publicly available and that inform the public, on an aggregate level, about: data sharing, data trends, Software adoption, and success in achieving Objective(s); additionally, Consultant shall be transparent about legal requests from government and non-government actors for the disclosure of User information and any responses to such requests.

2.6.3 Client shall make a Privacy Impact Assessment, as specified in section 2.10 below, publicly available prior to the deployment of the Software for public download and use.

2.6.4 The Parties shall ensure Users are notified when Software either achieves its Objective(s) or Software is unable to achieve Objective(s) so they may take steps to uninstall or otherwise deactivate the Software.

2.6.5 Software will use an openly published protocol to ensure that the source code is verifiable and interoperable, located at _____. Software source code shall be available under an open license so that the public can collaboratively inspect and address security shortcomings.

2.6.6 At least 72 hours prior to deploying Software or new versions or significant updates, the full source code, hardware, and/or firmware designs should be publicly available for evaluation. A full protocol specification should be available, including test data. An independent security audit of the source code by a reputed security representative should also be available and publicly announced alongside the announcement of the update.

2.7 Data Integrity

Consultant and Client will endeavor to ensure the Software operates in a manner that results in data that is accurate, updated, complete, of an appropriate quality for the Objective, and preserves data integrity.

2.8 Nondiscrimination

The Parties also agree to take steps to ensure that the Software does not Process Personal Data or generate data in a manner that perpetuates data inaccuracies, biases, or discrimination.

2.9 Accountability

Client shall ensure appropriate mechanisms to monitor compliance with Data Protection Law and this DPA, and provide meaningful avenues for individuals to lodge complaints and seek redress.

2.9.1 The Parties shall each appoint a privacy officer or other personnel responsible for ensuring compliance with Data Protection Laws, this DPA, processing and ensuring data subject rights, and responding to data protection complaints. For Client: _____; for Consultant: _____.

2.9.2 Client shall appoint an Independent Privacy, Civil Liberties and Data Ethics Advisory Board to oversee the planning and deployment of Software.

2.9.3 At Client's written request, Consultant shall make available to Client all information necessary to demonstrate compliance with Consultant's obligations under this DPA and applicable Data Protection Law, and to allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client.

2.10 Privacy Impact Assessment

Prior to the deployment of Software, Consultant and Client shall complete a privacy impact assessment ("PIA") that shall, at minimum, include the following:

2.10.1 For each item of Personal Data collected: describe the planned use of the data, retention period, path of transit, storage location(s), level of integration with other systems, whether automated decision-making will be applied, and identification of all entities who will access the Personal Data;

2.10.2 Draw a flowchart of the Software system;

2.10.3 Identify the privacy risks;

2.10.4 Identify measures to address or appropriately mitigate identified risks, including policies and procedures designed to ensure user privacy, data confidentiality, and system security;

2.10.5 Consultant and Client shall review, acknowledge and accept the PIA;

2.10.6 Provide an explanation of the privacy risks and mitigation safeguards in the applicable privacy disclosures; and

2.10.7 Ensure that the PIA is updated whenever there are material changes to the data practices, law or use of the Software, and maintain a copy of all prior versions of the PIA.

2.11 Security by Design

Parties shall take appropriate technical and organization measures to design the Software to operate with and be protected by reasonable information security, and to otherwise take reasonable steps to prevent the unauthorized or unlawful processing of Personal Data collected or processed by the Software. Consultant shall promptly, but in no less than 72 hours, notify Client upon becoming aware of a Data Security Incident and cooperate with Client in investigating, containing and remediating the Data Security Incident.

3. User Personal Data Rights[4]

3.1 Reasonable Steps to Ensure User Personal Data Rights

Client and Consultant will take reasonable steps to ensure the User Personal Data Rights specified herein.

3.2 User Personal Data Rights

In addition to any other data protection rights provided to Users by Data Protection Law, Users shall have the following personal data rights

3.2.1 The Right to Participate Voluntarily. User participation in Software shall be voluntary, based on informed, express, opt-in consent, and Users shall have a right to opt-out of use of the Software at any time.

3.2.2 The Right to Exercise Choice. Software shall provide users with choice regarding Personal Data collection, sharing, and use that is consistent with the context

in which it was collected and processed in the Software, unless otherwise required by law.

3.2.3 The Right to Be Informed. Users shall have the right to be informed about the data practices of the Software, including Personal Data collection, disclosures, and uses, as well as User privacy rights, through clear, conspicuous, meaningful and accessible privacy disclosures before their Personal Data has been collected.

3.2.4 The Right to Request Access. Users shall have the right to know what Personal Data has been shared with any third party, including the Client or any other governmental entity, unless such access is prohibited by law, would infringe upon the privacy interests of a third party, or would threaten public health needs.

3.2.5 The Right to Request Correction. Users shall have the right to correct their Personal Data if it is inaccurate, unless correction is prohibited by law, or would threaten public health needs.

3.2.6 The Right to Request Deletion. Users shall have the right to have their Personal Data deleted, unless retention of the data is mandated or expressly authorized by law, or deletion would threaten public health needs.

3.2.7 The Right to be Free from Discrimination. Users shall have the right to not be discriminated against for exercising their personal data rights, and to be free of bias and discrimination in the processing of their Personal Data.

4. Data Use[5]

4.1 Consultant Processing of Client Data

Consultant will process Client Data only at the instruction of the Client for the following purposes: (i) to provide the Software in accordance with this DPA and any other related or incorporated services agreement or statement of work; (ii) to perform any steps necessary for the performance of the Software; (iii) to response to verified data privacy rights request by User of the Software as directed by Client; and (iv) to comply with other reasonable, documented instructions provided by Client that are consistent with the DPA and applicable law. Consultant shall not collect, process or maintain Personal Data for any purpose outside those which are necessary to provide the services pursuant to this DPA.

4.2 Creation of Deidentified Data

Except as otherwise limited by this DPA, Consultant may use or disclose Client Data to create Deidentified Data, including for analytics purposes and to provide for the reports specified in section 2.6, as long as such use or disclosure of Client Data would not violate Data Protection Law or applicable privacy policies and commitments, and adheres to current best practices for the safe deidentification of data.

4.3 Consultant Data

Notwithstanding the foregoing and anything to the contrary in any applicable related services agreement or statement of work(including this DPA), Client acknowledges that Consultant will have a right to use and disclose Consultant Data for its own legitimate business purposes, as contemplated by any applicable related services agreement or statement of work, including to manage the relationship with Client, for billing, tax, and compliance purposes, to enforce applicable terms of service, protect its rights and property, to prevent fraud or misuse of the Software, to secure, maintain and improve the Software (for the benefit of Client and other customers engaged as clients for similar Software) and to monitor and analyze its activities in connection with the performance of the Software. To the extent Consultant Data is considered Personal Data, Consultant shall process such data in accordance with applicable Data Protection Laws, this DPA, and the applicable Privacy Policy.

5. Service Providers

5.1 Disclosure of Data to Third Parties

Consultant shall not disclose or transfer Personal Data to, or allow access by, any third party (including affiliates and subcontractors) without the express prior written agreement of Client, except where such disclosure, transfer or access is required by this DPA or applicable law (subject to Consultant providing Client with prompt written notice of such requirement to transfer or disclose, unless such notice is prohibited by applicable law). If Client approves Consultant’s use and/or transfer granting access of Personal Data to a third party, such third party shall, prior to any such disclosure, have entered into a data protection agreement at least as restrictive as this DPA. Such agreement shall be provided to Client promptly upon request. Consultant shall remain accountable and responsible for all actions by such third party subcontractors with respect to the disclosed or transferred Personal Data.

IN WITNESS WHEREOF, the Client and the Consultant have executed this DPA effective as of the date set forth above.

For Client

By: _____
Name: _____
Title: _____

For Consultant

By: _____
Name: _____
Title: _____



U.S. Digital Response would like to thank Colleen Brown, Dean Forbes and Michael R. Roberts at Sidley Austin LLP for their contributions and support in developing this model Data Protection Agreement.

To learn more about U.S. Digital Response, check out their website www.usdigitalresponse.org, contribute to their GitHub Repository, or follow them on twitter @USDResponse!

Footnotes

1. ***Drafting Note***: The model DPA was created with the intent of the Client being a local or state government; however, the DPA includes many generally applicable principles that may be appropriate for consideration in an agreement between purely private entity parties' development of exposure alerting applications and systems. Please note, however, that these model provisions do not constitute legal advice, and are not intended to be used as a replacement for advice of counsel. ↩

2. ***Drafting Note***: Some defined terms will be general, such "Data Protection Law," while others will arise from the specific services provided, for example the terms "Client Data" and "Consultant Data." ↩

3. ***Drafting Note:*** The Purpose is the overarching reason why the software is necessary, whereas an Objective is a specific goal that the Software will achieve. For example, a Purpose for the Software may be to provide Users with risk-based information that they can use to assess their personal health and direct them to seek medical assistance. An Objective that relates to that Purpose is to create a system to securely store mobile phone data that can alert Users if they've been in proximity of a person with COVID-19. A separate Objective would be to collect User data that will assist public health officers in manual contact tracing. ↩

4. ***Drafting Note:*** The parties will need to provide a mechanism for the exercise of user rights, such as a web form, telephone number, or email address where users can make requests. ↩

5. ***Drafting Note***: The rights and responsibilities that the parties have with regards to the User data collected by the Software will need to be more clearly defined. This provision establishes that Consultant will provide the infrastructure on which the User Data will be stored as a service provider to Client, and that Client will be the data custodian of the User Data. ↩