GDPR Checklist

Prepared by the Stoel Rives Privacy and Data Security Group

Note to Readers: *This Checklist is designed to assist companies wishing to comply with the General Data Protection Regulation ("GDPR"), which becomes applicable May 25, 2018. Please direct specific questions about GDPR compliance to one of the members of our team:*

Amy Carlson: amy.carlson@stoel.com

Hunter Ferguson: hunter.ferguson@stoel.com

Wally Van Valkenburg: wally.vanvalkenburg@stoel.com

Caution: *This checklist does not constitute legal advice. The GDPR contains a complex set of rules, and this checklist is only a summary of the rules.*

No one-size-fits-all template exists for privacy programs. When a company begins the process of developing a privacy program, it should consider matters such as how the company collects personal information, the purposes for which it collects the information, who requires access to the information, how the company uses or may wish to use the information, how long the company needs to maintain the information, and how the company stores and disposes of the information.

Successful privacy compliance programs are based on a culture of compliance, which requires buy-in and direction from senior management. The compliance program should be structured to create a broad awareness within the Company of key privacy issues and the importance of addressing them throughout the business as they arise. Privacy is cross-functional and must be coordinated with stakeholders across the company.

GDPR Checklist

1. Does GDPR apply?

GDPR applies to the processing of personal data by Controllers and Processors with an EU presence regardless of whether the processing takes place in the EU or not. It also applies to the processing of personal data of Data Subjects in the EU by a Controller or Processor not established in the EU where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU.

2. If GDPR applies, what do we need to do to comply?

(a) Adopt and enforce GDPR compliant policies

(b) If necessary, appoint a Data Protection Officer

(c) If necessary, appoint an EU representative

(d) Implement privacy by design

(e) Implement appropriate data security measures

(f) Implement appropriate breach notification measures

(g) Maintain required documentation

(h) When necessary, complete a Data Protection Impact Assessment

(i) Execute an appropriate Data Processing Addendum with any entity that processes Personal Data for the Company or for whom the Company processes Personal Data.

3. Adopt and enforce GDPR compliant policies

3.1 Internal and external policies. GDPR requires that companies abide by certain general principles in processing Personal Data, that they have a lawful basis for processing that data, that they provide Data Subjects with certain information when they collect Personal Data, and that they extend certain rights to the Data Subjects. The Company should develop and adopt both an internal Compliance Policy that documents the Company's compliance with these requirements and an external Privacy Policy that provides Data Subjects with the required information and disclosures.

3.2 General Principles. GDPR requires that companies adhere to the following general principles in processing Personal Data:

- **Lawfulness, fairness and transparency.** The Company must process all Personal Data lawfully, fairly and in a transparent manner in relation to the Data Subject.

- **Purpose limitation.** The Company must process Personal Data only for specified, explicit and legitimate purposes.

- **Data minimization.** The Company must collect and maintain Personal Data only to the extent necessary in relation to the purpose for which it is processed.

- **Accuracy.** The Company must use commercially reasonable efforts to ensure that any Personal Data it maintains is accurate and up to date. The Company must use commercially reasonable efforts to correct or erase Personal Data which is inaccurate.

- **Storage limitation.** The Company must not maintain Personal Data in a form that permits identification of Data Subjects for longer than is necessary for the purpose for which the data was processed.

- **Integrity and confidentiality.** The Company must use reasonable efforts, including use of appropriate technical and organizational security measures, to ensure appropriate security of Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

- **Accountability.** The Company must create and maintain systems that enable it to demonstrate compliance with the data protection principles set forth above.

3.3 Lawful Basis for Processing. GDPR requires that the Company have a lawful basis for processing Personal Data. The lawful bases for processing are:

- **Consent.** The Data Subject has given consent.

- **Performance of Contract.** Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract

- **Compliance with Legal Obligation.** Processing is necessary for compliance with the Controller's legal obligations

- **Protection of Vital Interests.** Processing is necessary in order to protect a person's "vital interests"

- **Public Interest.** Processing is necessary for a task carried out in the public interest or in the exercise of the Controller's official authority

- **Legitimate Interests of Controller.** Processing is necessary to protect the legitimate interests of the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

3.4 Obtaining Consent. Where the Company requests a Data Subject's consent to the processing of Personal Data, the request must be made in plain language that is intelligible and easily accessible. The request must state the purpose for the processing and that the

consent may be withdrawn at any time. The request must also require an affirmative indication of consent by the Data Subject, including by way of example checking a box on a website or in an app. If consent is requested in a written document that also concerns other matters, the request for consent must be presented in a way that is distinguishable from the other matters.

3.5 Right to Information. If the Company collects Personal Data directly from a Data Subject, the Company must provide the Data Subject with the following information:

- Company's name and contact details and, where applicable, its representative.
- If the Company maintains a Data Protection Officer, contact details for the Data Protection Officer.
- The intended purposes of, and the legal basis for, the processing.
- Where the processing is based on the Company's legitimate interest, what that legitimate interest is.
- The recipients or categories of recipients of the Personal Data, if any.
- If the Company intends to transfer the Personal Data to a recipient in a country outside the EEA, the existence or absence of a Commission adequacy decision or information about the appropriate or suitable safeguards adduced to secure the data and the means to obtain a copy of them or where they have been made available.
- The period for which the data is stored, or the criteria used to determine that period.
- The existence of the Data Subject's rights of access, rectification, erasure, restriction of processing, to object to processing, and to data portability
- Where processing is based on the Data Subject's consent, the right to withdraw that consent at any time.
- The right to lodge a complaint with the Supervisory Authority.
- Whether the provision of Personal Data is a statutory or contractual requirement or a requirement necessary to enter into a contract. The Data Subject must be informed about any obligation to provide Personal Data and of the consequences of a failure to do so.
- The existence of automated decision-making or profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

If the Company does not collect the Personal Data from the Data Subject, the in additional to the information described above, the Company must provide the Data Subject with the following additional information:

- The categories of personal data concerned

- From which source the Personal Data originate and, if applicable, whether it came from Publicly accessible sources

3.6 Right to Data Erasure. Upon request from a Data Subject, the Company must erase his/her Personal Data and cease further dissemination of the data if any of the following apply:

- The data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

- The Data Subject withdraws consent on which the processing is based, and there is no other legal ground for the processing of the data.

- Where the ground for processing is the public interest or the interest of the Company or a third party, the Data Subject objects to the processing of Personal Data and there are no overriding legitimate grounds for the processing.

- The Data Subject objects to the processing of the data for direct marketing purposes (including profiling to the extent that it is related to direct marketing).

- The Personal Data has been unlawfully processed.

- The Personal Data is required to be erased to comply with applicable law.

- The Personal Data has been collected in relation to paid online services offered directly to a child.

If the Company is required to erase Personal Data, the Company must also inform other controllers to whom the Personal Data has been disclosed that the Data Subject has requested erasure by them of any links to, or copies of, that data.

The Company is not required to erase data or inform third party controllers of the Data Subject's request to the extent that the processing is necessary for any of the following reasons:

- Exercising the right of freedom of expression and information.

- Compliance with a legal obligation under applicable law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- For reasons of public interest in the area of public health.

- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.

- For the establishment, exercise or defense of legal claims.

3.7 Additional Data Subject Rights. In additional to the rights to information and data erasure described above, GDPR requires that the Company recognize the following Data Subject rights:

- **Right to Access.** The Company must inform a Data Subject upon request whether or not his or her Personal Data is being processed, where, and for what purpose. Upon request, the Company must also provide a copy of the Personal Data, free of charge, in an electronic format.

- **Right to Rectification.** In the event the Company determines that Personal Data is inaccurate or incomplete, the Company must correct or complete the Personal Data as applicable.

- **Right to Restrict Processing.** Upon request by a Data Subject, the Company must restrict processing of the Data Subject's Personal Data where: (a) the Data Subject contests the accuracy of the Personal Data; (b) the processing is unlawful and the Data Subject opposes erasure and requests restriction instead; (c) the Controller no longer needs the data for processing, but the data is required by the Data Subject in connection with legal claims; or (d) the Data Subject has objected to processing, the ground for processing is the public interest or the interest of the Company or a third party, and there are no overriding legitimate grounds for the processing.

- **Right to Data Portability.** Upon request from a Data Subject, the Company must provide the Data Subject with Personal Data the Data Subject has previously provided to the Company. The Company must provide the information in a commonly used and machine readable format and, upon request from the Data Subject, must transmit that data to another Controller.

- **Right to Object.** If the Data Subject objects to processing of his or her Personal Data, and the ground for processing is the public interest or the interest of the Company or a third party, the Company must cease processing unless there are overriding legitimate grounds for the processing.

3.8 Minors. GDPR prohibits processing Personal Data of children below the age of 16 unless the child's parent consents.

3.9 Special Categories. GDPR prohibits processing of the following categories of Personal Data ("Special Categories") unless certain conditions are met: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." Generally speaking, such processing is permissible in fewer situations than is true for other categories of Personal Data.

3.10 Criminal Convictions and Offenses. GDPR provides that processing of Personal Data relating to criminal convictions and offenses "shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects."

3.11 Adoption and Implementation of Policies. Both the Compliance Policy and the Privacy Policy should be adopted by the Board of Directors or senior management of the Company and distributed to all appropriate personnel. Once adopted by the Company, the commitments become enforceable under U.S. law.

4. If necessary, appoint a Data Protection Officer

4.1 Under the GDPR, a company must appoint a "Data Protection Officer" ("DPO") if the company carries out: (1) large scale systematic monitoring of individuals (for example, online behavior tracking); or (2) large scale processing of Special Categories of data or data relating to criminal convictions and offenses.

4.2 If a DPO is required, the DPO must: (a) inform and advise the Company and its employees about their obligations to comply with applicable data protection laws; (b) monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits; and (c) be the first point of contact for supervisory authorities and for individuals whose data is processed, including employees and customers.

4.3 The DPO must: (a) report to the highest management level" of the Company; (b) operate independently and be protected from dismissal or penalization for performing his or her duties; and (c) be afforded adequate resources to perform his or her duties. The DPO must have professional experience and knowledge of data protection law proportionate to the type of processing the Company carries out, taking into consideration the level of protection the Personal Data requires.

4.4 If a DPO is required, contact details for the DPO must be provided to the applicable Supervisory Authority in the EU.

5. If necessary, appoint a representative

5.1 The GDPR requires Controllers and Processors who are not resident in the EU to "designate in writing a representative in the Union."

5.2 Such a designation is not required for: (a) processing which: (1) is occasional; (2) does not include, on a large scale, processing of Special Categories of data or data relating to criminal convictions and offenses; and (3) is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body.

5.3 The Data Protection Officer and Designated Representative may but need not be the same person. If the Company does not have a physical presence in the EU but is required to have a Designated Representative, the Data Protection Officer and Designated Representative are likely to be different persons because the DPO should be resident at the Company's principal place of business.

6. Implement privacy by design

6.1 GDPR requires a Company to use reasonable efforts to implement data protection measures by design and default when processing Personal Data. The Company

must implement appropriate technical and organizational measures to ensure compliance with data protection principles.

6.2 In considering and implementing privacy by design, the Company must take into account the following:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purposes of processing.
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

6.3 The Company must take measures to ensure that, by default, the Company processes only Personal Data that is necessary for the specified purpose. Such obligation must apply to the amount of Personal Data collected, the extent of its processing, the period of its storage, and its accessibility. The Company must at all times, by default, protect Personal Data from unauthorized sharing with an indefinite number of third parties.

7. Implement appropriate data security measures

7.1 The Company must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected. The Company must ensure that its employees and others acting under its control who have access to Personal Data do not process it except in accordance with such measures or as required by applicable law. Measures the Company may take to secure Personal Data include the following:

- The pseudonymisation and encryption of Personal Data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

7.2 When assessing the appropriate level of security for Personal Data, the Company must take into account:

- The nature, scope, context and purposes of processing
- The risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data.

8. Implement appropriate breach notification measures

8.1 In the event the Company learns of a Personal Data Breach, except as otherwise provided below, the Company must:

- Notify the Company's Supervisory Authority within 72 hours of becoming aware of the breach
- Notify any Data Subjects whose Personal Data was affected without undue delay

If the Company is required to notify a Supervisory Authority, the notice must:

- Describe the nature of the breach, including the categories and number of Data Subjects concerned, and the categories and approximate number of data records concerned.
- Communicate the identity and contact details of the DPO or other contact point where more information can be obtained.
- Describe the consequences of the breach.
- Describe the measures proposed or taken by the Company to address the breach.

8.2 If the Company is required to notify Data Subjects of a breach, the notice must:

- Describe the nature of the breach.
- Provide the name and contact details of the DPO or other contact point.
- Describe the consequences of the breach.
- Described the measures proposed or taken by the Company to address the breach.

8.3 The Company is not required to notify the Supervisory Authority or any Data Subjects if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

8.4 The Company is not required to notify Data Subjects of the breach if any of the following conditions are met:

- The Personal Data was encrypted or otherwise subject to protection measures that render the data unintelligible to unauthorized persons.
- The Company has taken subsequent measures to ensure that high risks to the rights and freedoms of Data Subjects are unlikely to materialize.
- Notice would involve a disproportionate effort (in which case the Company must provide a public communication or similar measure to inform the affected Data Subjects in an equally effective manner).

9. Maintain required documentation

9.1 Company Processing. The Company must maintain a record of all processing operations under its responsibility, which record must include the following:

- The name and contact details of the controller, or any joint controller or processor, and of the Designated Representative, if any.
- The name and contact details of the DPO, if any.
- The purposes of the processing.
- A description of categories of Data Subjects and of the categories of Personal Data relating to them.
- The recipients or categories of recipients of the Personal Data, including recipients in third countries or international organizations.
- Where applicable, transfers of data to a third country or an international organization, including the identification of that third country or international organization. In the case of transfers that include one-off or infrequent processing of limited amounts of Personal Data in the legitimate interest of the data controller or processor, the appropriate safeguards must also be documented.
- Where possible, a general indication of the time limits for erasure of the different categories of data.
- Where possible, a description of the technical and organizational security mechanisms the data controller employs.

9.2 Third Party Processing. If the Company processes data for a third party, the Company must maintain a record of all processing activities carried out on behalf of the third party, which record must include the following:

- The name and contact details of the processor or processors and of each controller on behalf of which the controller is acting, and of the controller's representative (if any).
- The name and contact details of the processor's DPO, if any.
- The categories of processing carried out on behalf of each controller.
- Where applicable, the categories of transfers of Personal Data to a third country or an international organization.
- Where possible, a general description of the data security measures put in place by the processor.

10. When necessary, complete a Data Protection Impact Assessment

10.1 When required. GDPR requires the Company to complete a Data Protection Impact Assessment ("DPIA") prior to engaging in any of the following activities:

- Profiling, or any other automated form of processing of Personal Data for the purpose of evaluating personal aspects of the Data Subjects.
- Processing Special Categories of data or data relating to criminal convictions or offenses on a large scale.
- Systematic monitoring of a publicly accessible area on a large scale (for example, through video surveillance or closed-circuit television).

10.2 Contents. In the event the Company is required to conduct a DPIA, the DPIA must include the following:

- A systematic description of the processing operations and the purposes of the processing, including the legitimate interest to be pursued.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of the Data Subjects.
- The measures the Company intends to take to address the risk, including safeguards, security measures, and mechanisms, to ensure the protection of the Personal Data collected.

11. Execute an appropriate Data Processing Addendum with any entity that processes Personal Data for the Company or for whom the Company processes Personal Data.

11.1 If the Company transfers Personal Data to third-party agents or service providers who perform functions on the Company's behalf, or if it receives such information as a Processor, the Company must enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the Company's policies require and limiting their use of the data to the specified services. The Company must take reasonable and appropriate steps to ensure that the third-party agents and service providers process the Personal Data in accordance with Company policies and that they stop and remediate any unauthorized processing.

11.2 If Personal Data is transferred outside of the EU, the European Commission must find that the protections available in the transferee country are essentially equivalent to those required by the EU and provide Data Subjects with effective enforcement mechanisms. In the absence of an adequacy determination, transfers of Personal Data can be made where the data recipient has provided adequate safeguards for the rights of the Data Subject. Safeguards may be provided by way of, among other mechanisms, binding corporate rules adopted by the recipient or standard contractual clauses adopted or approved by the Commission, an approved code of conduct, or an approved certification mechanism.

12. Definitions.

As used in this Checklist, the following terms have the following meanings:

"Controller" means any person or organization that collects Personal Data and that determines the purpose for and means of processing the data.

"Data Protection Officer" means a person designated by the Company to oversee implementation and enforcement of the policies set forth in this Manual.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates. A person is "identifiable" if he or she can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"Designated Representative" means a natural or legal person designated by the Company who is established in one of the Member States where Data Subjects are located whose Personal Data is processed or whose behavior is monitored.

"Member States" means countries that are members of the European Union.

"Personal Data" means information relating to a Data Subject. Types of personal data include name and surname; a home address; an email address such as name.surname@company.com; an identification card number; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; the advertising identifier of your phone; and data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Company.

"Process" or "processing" of data means any operation or set of operations on the data, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future), erasure and destruction.

"Processor" means any person or organization that processes data on behalf of the Company, including cloud service providers.

"Profiling" means automated processing of Personal Data to analyze or predict aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"Pseudonymisation" means the separation of data from direct identifiers of a Data Subject so that the Personal Data cannot be attributed to the Data Subject without additional information that is held separately.

“Special Categories” of data means Personal Data that reveals racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.

“Supervisory authority” means an independent public authority established by a Member State that is responsible for monitoring the application of applicable privacy laws and regulations.