Lessons Learned After One Year of GDPR

-GDPR Overview Handout-

FIRMA 2019 Orlando Conference

Justin P. Webb, CIPP/US

Godfrey & Kahn S.C.

I. Introduction to the GDPR

a. The European Union's General Data Protection Regulation (Regulation (EU) 2016/679)

b. Went into effect May 25, 2018

c. Governs the Processing of Personal Data

i. Personal Data means "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

ii. Note: specific rules apply to the processing of sensitive Personal Data, including "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 shall be prohibited."

iii. Processing means "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."

d. Replaced the EU's Privacy Directive 95/46/EC

e. The European approach to privacy is radically different from the traditional American approach because the EU treats privacy of information as a fundamental human right.

f. The GDPR caught the attention of many US companies for the first time due to the extra-territorial application and potentially large fines of up to 4% of revenue.

g. Despite passage in 2016, companies and regulators were not fully prepared for its implementation.

II. Who does it apply to?

a. The GDPR applies to entities inside and outside of the EU through Article 3

   i. "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

b. The GDPR applies to entities that:

   i. Are established in the EU

   ii. Offer goods or services into the EU

   iii. Monitor the behavior of individuals in the EU

c. The European Data Protection Board ("EDPB") issued draft guidance on the territorial scope of the GDPR. The guidance laid out three tests based upon Article 3: the Establishment Test, the Offering of Goods or Services Test, and the Monitoring Behavior Test.

   i. Establishment Test – Regulators and EU courts evaluate whether an entity has human and technical resources in the EU. Evaluations are very fact-specific.

   ii. Offering Goods or Services Test – Regulators and EU courts look at whether the entity "envisages" providing goods and services to EU individuals and whether the entity is targeting EU individuals specifically. The test is not based on whether an entity *actually* provides goods or services into the EU, but rather based on whether the entity *intends to provide* services or goods into the EU.

   iii. Monitoring Behavior Test – Regulators and EU courts focus on whether an entity is monitoring or tracking behavior of individuals in the EU for the purpose of profiling those individuals or advertising to them based on their online traffic. To satisfy the test, the entity must purposefully be collecting and reusing the Personal Data in an effort to target EU individuals.

III. Requirements of the GDPR

a. Legal basis of processing (Article 6)

   i. Entities must process data under one of the following legal basis:

      1. The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes;

      2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

      3. Processing is necessary for compliance with a legal obligation to which the controller is subject;

      4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

      5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

      6. Processing is necessary for the purposes of the legitimate interests pursued by 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.

   ii. Companies should avoid using consent as a legal basis because consent must be informed and affirmative and may be revoked.

b. Data subject rights (Articles 12-23)

   i. Right of access

   ii. Right to rectification (correction)

   iii. Right of erasure (right to be forgotten)

   iv. Right of data portability

   v. Right of restricted processing

   vi. Right to lodge a compliant

c. Notification requirements (Articles 12-14)

i. Where Personal Data relating to a data subject are collected from the data subject, the controller shall, at the time when Personal Data are obtained, provide the data subject with all of the following information:

1. The identity and the contact details of the controller and, where applicable, of the controller's representative;

2. The contact details of the data protection officer, where applicable;

3. The purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;

4. Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

5. The recipients or categories of recipients of the Personal Data, if any;

6. Where applicable, the fact that the controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

ii. In addition to the information referred to in paragraph 1, the controller shall, at the time when Personal Data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

1. The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

2. The existence of the right to request from the controller access to and rectification or erasure of Personal Data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

3. Where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

4. The right to lodge a complaint with a supervisory authority;

5. Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the Personal

Data and of the possible consequences of failure to provide such data;

6. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

iii. Privacy policies or notices must be concise, transparent, and easily readable.

d. Transfer limitations (Articles 44-50)

i. Entities must have transfer mechanism to transfer Personal Data outside of the EU, such as:

1. An adequacy decision for the country to which it is being transferred

2. Adequate safeguards in the form of binding corporate rules, approved codes of conduct/certifications, or standard contractual clauses

3. Specific derogations for occasional transfers:

a. The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. The transfer is necessary for important reasons of public interest;

e. The transfer is necessary for the establishment, exercise or defence of legal claims;

f. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g. The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

e. Mandatory contracting (Articles 24-28)

i. The GDPR requires a written contract between controllers and processors.

1. A controller "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

2. A processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

3. The EDPB has adopted previous guidance issued by the previous EU regulation body (Article 29 Work Party) on how to determine when an entity is a controller versus a processor.

ii. Article 28 requires that the contract includes the following:

1. Processes the Personal Data only on documented instructions from the controller, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

2. Ensures that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. Takes all measures required pursuant to Article 32;

4. Respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

5. Taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's

obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

6. Assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

7. At the choice of the controller, deletes or returns all the Personal Data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data;

8. Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

f. Records of Processing (Article 30)

i. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

1. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

2. The purposes of the processing;

3. A description of the categories of data subjects and of the categories of Personal Data;

4. The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;

5. Where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

6. Where possible, the envisaged time limits for erasure of the different categories of data;

7. Where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

ii. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data. A single assessment may address a set of similar processing operations that present similar high risks.

iii. The controller and the processor shall designate a data protection officer in any case where:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

2. The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or Personal Data relating to criminal convictions and offences referred to in Article 10.

g. Breach reporting and notice obligations (Articles 33-34)

i. In the case of a Personal Data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the supervisory authority competent in accordance with Article 55, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ii. When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the Personal Data breach to the data subject without undue delay.

h. Appropriate data security (Article 32)

i. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. The pseudonymisation and encryption of Personal Data;

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

IV. The GDPR, One Year In

a. EU regulators have focused enforcement efforts on either global technology companies or egregious violations. Twitter, Facebook, and Google have all faced a large amount of scrutiny by EU regulations. Google received a $57 million fine from the French Data Protection Authority for not properly disclosing to users how Personal Data was collected.

b. EU regulators are using their investigation powers and are issuing orders for companies to take certain actions, such as ceasing to process Personal Data.

c. The fines issues thus far have generally been on the lower end. Regulators are issuing fairly small fines to companies that cooperate with the regulator.

d. To date, there have been no attempts to reach across to US companies that are not otherwise established in the EU.

e. A recent UK Data Protection survey conducted partly by the Information Commissioner's Office ("ICO") found that a large percentage of organizations still had not appointed an individual or a team to assume responsibility for complying with data protection laws. 10% reported having no privacy policies at all. 15% stated they had no processes in place to handle a data breach. Only 46% stated they had documented processes to maintain records of processing.

f. GDPR may impact the availability or process of discovery. The Northern District of California held that GDPR did not preclude the Court from ordering a defendant to produce un-redacted emails. Finjan, Inc. v. Zscaler, Inc., 2019 WL 618554, No. 17-cv-06946-JST (N.D. Cal. Feb. 2, 2019).