Guidelines for Data Protection Impact Assessments under the GDPR[1]
November 2018

Data Protection Impact Assessments (DPIAs) are required by the EU General Data Protection Regulation (GDPR) as a way to demonstrate that companies are managing the risks associated with their processing of personal data. GDPR Article 35[2] provides that controllers must assess the impact of any processing activities where the processing is **likely to result in a high risk** to the rights and freedoms of natural persons, in particular where new technologies are used. In determining whether a DPIA is needed, controllers must consider the nature, scope, context and purposes of the processing, as well as the specific cases where DPIAs are required by the law, namely:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of data referred to in Article 9(1) or of personal data relating to criminal convictions and offences; or

c) systematic monitoring of a publicly accessible area on a large scale.

The Article 29 Working Party Guidelines on Data Protection Impact Assessments[3] (WP 248 rev.01, 4 October 2017 and endorsed by the European Data Protection Board) provide additional information regarding the types of processing activities that would generally necessitate a DPIA triggers. The Guidelines delineate the following nine criteria that should be considered when determining if a DPIA is needed. We can use these criteria to create a list of "Additional Risk Factors" that will influence the decision regarding whether a DPIA is needed. These Additional Risk Factors are:

1. Any processing of personal data for **evaluation or scoring** (including profiling and predicting);
2. Any **automated decision-making with legal or similar significant effect**;
3. Any **systematic monitoring** (meaning any processing used to observe, monitor or control data subjects);
4. Any processing of **sensitive data** or data of a highly-personal nature;
5. Any **large scale** processing of personal data or processing a **large volume** of personal data;
6. Any **matching or combining datasets** if the data were (for example) collected for different purposes or by different controllers in a way that the data subjects would not reasonably expect;
7. Any processing of personal data concerning **vulnerable data subjects** (children, employees, patients, elderly persons, mentally-ill persons, asylum seekers, etc.) or any case where there is an i**mbalance in the relationship** between the controller and the data subjects;
8. Any use of **innovative technologies** (such as combining facial recognition with fingerprint recognition for access controls or Internet of Things applications with connected devices that collect personal data); or
9. Any **processing that in itself prevents a data subject from exercising a right or using a service,** such as automated access systems or credit scores.

---

[2] See GDPR Article 35: http://www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm

[3] https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_en

This Guideline is designed to establish specific DPIA triggers within Acme. Our goals are both to comply with GDPR and also to allow us to properly identify and manage privacy risks. If you have any questions about whether to conduct a DPIA (or about the evaluation of privacy risks when completing the DPIA), please contact the [Acme Data Protection Officer].

1. Mandatory DPIAs

Always complete a DPIA if the processing activity is likely to result in high risk for the individuals. The following activities always require a DPIA:

- Any profiling or automated decision-making that is used to make significant decisions about people. For example:
  - Automated customer qualification or price-setting processes, such as those that use credit scores,
  - Employee background screening programs,
  - Automated employee monitoring programs,
  - Automated security or loss prevention programs, such as call center analytics to detect fraud, or
  - Any other program that would result in an automated decision that prevents an individual from using a service or system.

- Any large scale processing of sensitive personal data, namely those data elements that reveal race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, physical or mental health, or that include genetic data, biometric data or records relating to criminal offenses or allegations of crimes. This includes projects that infer these data elements. For example:
  - Systems that process special categories of data, *e.g.* healthcare patient data or criminal records,
  - Employee health and wellness programs,
  - Criminal records checks and watch list screening programs,
  - Whistleblower programs,
  - Diversity programs,
  - Occupational safety programs and public health programs, or
  - Security programs, such as authentication/identification programs using biometric identifiers.

- Any large scale, systematic monitoring of publicly-available areas. For example:
  - Audio or video surveillance of public areas (parking lots, building lobbies, elevators, *etc.*),
  - Automatic vehicle license plate number recognition systems,
  - Traffic management systems involving monitoring of vehicle or driver behavior,
  - Wi-Fi, Bluetooth and RFID tracking, or
  - Online scanning for company, intellectual property or reputational issues.

- Any large scale profiling of individuals, meaning any automated processing of personal data that analyzes or predicts any aspects of a person's performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements, including profiling for:
  - Marketing or loyalty programs,
  - Social media campaigns or interest-based ad targeting,
  - Product development, research or analytics,
  - Fraud detection and prevention or other security purposes, or
  - Human resources purposes, such as to generate success scores or to evaluate flight risk or compliance risk.

- Large-scale tracking, such as:
  - Online tracking, such as to determine effectiveness of online advertising or to support delivery of interest-based ads,
  - Tracking or telematics via IoT devices, sensors, applications and platforms,
  - Mobile and cross-device tracking,
  - Online engagement tracking, such as eye tracking or mouse movement analytics,

  - Location tracking, including tracking employees using GPS or mobile device data, or
  - Tracking in retail stores to determine in-store behavior.

- Use of biometric data (such as biometric timeclocks or access systems, fingerprint readers, facial recognition or voice recognition systems) or genetic data, if the data are used for individual identification.

- Any processing activities that involve two or more of the Additional Risk Factors set forth above, such as:
  - Machine and deep learning or natural language processing algorithms, including AI-based customer service, with any other Risk Factor (e.g.,) if the application is large scale, involves profiling, or is used with a vulnerable population;
  - Precise location data processed with any other Risk Factor, such as for systematic monitoring or concerning children or the elderly;
  - Data processed by smart meters or IoT applications, including remote metering systems that allow profiling or systematic monitoring of individuals or groups of people;
  - Systems that transmit senor or smart meter data to us or other third parties via mobile apps or communications networks, such as devices that "phone home" to Acme;
  - Systems that analyze or process data located in metadata (such as geolocation data in images),
  - Other smart technologies, including wearables, if they collect any sensitive data or may be used by vulnerable individuals;
  - Matching datasets, if the data are sensitive or pertain to vulnerable individuals, or in any case where the data subjects would not reasonably expect the data to be combined;
  - Other analysis tools for personal data, such as automated analysis of video or audio recording for sentiment analysis, fitness/lifestyle monitoring, productivity analytics, *etc.;* or
  - Any devices or technologies that could endanger an individual's health if there was an incident.

2. Recommended DPIAs

Consider completing a DPIA if the processing activity could result in real risk to an individual. A DPIA is always appropriate if the risks associated with a project could result in real risk, so that we can document that the risks are appropriately mitigated. A DPIA can also help us understand risks that might not have been considered by the project team. Data protection authority guidance in some countries recommends DPIAs for these activities as well.

Examples of projects where a DPIA should be considered:

- Data matching (cross-referencing data sets) or combining data from different sources, such as
  - Data enhancement projects for direct marketing, where Acme data are enhanced with third party data or social media data, or
  - Data enhancement or cross-referencing of employee data (such as for benefits utilization analytics or wellness programs).

- Smaller-scale or internal tracking,[4] such as:
  - Tracking of devices issued to employees for asset management or inventory control purposes,
  - Maintaining electronic physical access logs (such as automated visitor logs or to record employee access to secure areas, such as data centers), or
  - Audio or video surveillance of common areas within the facility.

- Any project that processes personal data of vulnerable individuals, such as children, the elderly, patients or disabled persons, including product development projects to accommodate these individuals.

[4] If the tracking project is large scale, you must complete a DPIA.

- Any project that involves collecting personal data from individuals who do not know that Acme is processing their data and who do not receive a privacy notice from us.

- Any project that entails providing a third party (including a processor) with access to sensitive personal data, particularly if the third party is another country or region.

3. DPIAs Not Required

A DPIA is not required if there is clearly no high risk to individuals from the processing. This means that DPIAs are not needed for many standard or routine business processing activities. For example:

- Processing prospective, current and former employee and family member data as needed for many customary human resources purposes (recruitment without automated decision-making, hiring, work eligibility, staffing, compensation and benefits, including social and health insurance) and for other legitimate purposes (such as time and expense management, non-biometric access control systems, badging, talent and performance development, training, oversight, succession planning and HR support services).

- Processing activities related to business transactions, such as non-automated customer or supplier qualification, transaction processing and fulfillment, finance functions (accounts payable and receivable, collections), quality control, product returns, enforcing contractual terms, non-marketing communications related to the transactions (such as order confirmations and shipping notices).

- Providing customer service, including non-marketing communications related to customer inquiries (such as responses to questions, requests for proposals or information and complaints) and dispute resolution.

- First party marketing and providing loyalty or rewards programs, with opt-in enrollment.

- Customary corporate functions, such as internal audit, reporting, and conducting corporate due diligence in connection with mergers and acquisitions.

- Data management, including data hygiene (updating records to improve accuracy), processing for minimization, pseudonymization, anonymization, or aggregation, and processing in connection with disaster recovery and business continuity purposes (including making back-ups, retention, archiving and data deletion).

- Analytics on transactional data (purchases, returns, *et al.*) to identify process or production weaknesses, customer satisfaction, opportunities for efficiency, improvement, and other purposes that do not entail profiling or monitoring of individuals.

- Processing activities needed for IT system administration and data security, including administering websites, device and application management, maintaining logs, cybersecurity controls and incident response programs with human oversight.

- Processing activities needed to comply with law, including tax and labor reporting, managing data subject rights requests and responding to personal data breaches.