The list of types of personal data processing operations, for which carrying out a Data Protection Impact Assessment (DPIA) is required

The following list contains the types of processing operations which in the opinion of the Personal Data Protection Office (Urząd Ochrony Danych Osobowych) require a DPIA. This list has been developed in order to fulfil the obligation imposed on the Personal Data Protection Office as the Polish supervisory authority under Article 35(4) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as GDPR. This list does not exempt the controller from the obligation to assess any processing operation based on complete Data Protection Impact Assessment under Article 35(1) of the GDPR. The relevant list is based on Article 29 Working Party's Guidelines (WP248) "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". This list complements and further specifies the aforementioned guidelines.

As a rule, the processing which meets at least two of the below mentioned criteria will require a DPIA. In some cases the data controller can, however, consider that the processing which meets only one of the below mentioned criteria will require a DPIA. The more criteria are met by the processing, the more likely it is to result in a high risk to the rights and freedoms of data subjects, and in consequence, regardless of the security measures envisaged for application by the controller, a DPIA will be required.

The Personal Data Protection Office emphasises that any examples of the existing areas of application have been provided exclusively for illustrative purposes, and in consequence "The examples of operations/ scope of data/ circumstances, in which specific type of operation is likely to result in a high risk" are not of exhaustive nature. The examples included in the list are only aimed to help in better understanding of the criteria/types of operations which are likely to result in the need to carry out a DPIA.

This list in no way undermines the general obligation of the controller to carry out a proper risk assessment and risk management. Carrying out a DPIA also does not exempt the controller from the obligation to comply with other obligations provided for in the GDPR or other obligations contained in other relevant provisions.

I. Types/criteria for processing operations, for which carrying out a DPIA is required	II. Potential areas of occurrence/existing areas of application	III. Examples of operations/ scope of data/circumstances, in which specific type of operation is likely to result in a high risk
1. **Evaluation or assessment, including profiling and prediction (behavioural analysis) for the purposes, which can produce <u>negative legal, physical and financial effects, or other inconveniences for individuals</u>**	Social media, marketing companies, headhunting companies.	Profiling of users of social networking sites and other applications for the purposes of sending them commercial information.
	Banks, other financial institutions authorized to grant loans, loan institutions in the process of assessing creditworthiness.	Creditworthiness assessment, with the use of Artificial Intelligence algorithms covered by the obligation of secrecy and requesting disclosure of data not directly related to creditworthiness assessment.
	Insurance companies – offering discounts related to lifestyle (cigarettes, alcohol, extreme sports, car driving).	Evaluation of individuals' lifestyle, diet, driving, leisure activities, etc. for the purpose for example of increasing the price of their insurance premium, based on this evaluation generally called optimising the insurance premium.
	Insurance companies – e.g. more favourable insurance or credit offers for employees of specific groups, e.g. public administration, teachers.	Indirect profiling (evaluation of an individual based on membership of a particular group).
2. **Automated decision-making <u>producing legal, financial or similar significant effects</u>**	Roads covered by SPECS (the system stores not only information on the vehicles violating the regulations, but also on all the vehicles appearing in the controlled area), selected road sections equipped with electronic toll collection system via TOLL.	Monitoring systems used for traffic management enabling detailed surveillance over each driver and his/her driving behaviour, in particular systems enabling automated identification of vehicles. Automated toll collection systems

	Online stores offering promotional prices for specific groups of customers. Companies that support loyalty programs (shopping communities)	Customers profiling systems in terms of identifying shopping preferences, automated setting promotional prices based on a profile.
	Marketing programmes containing elements of individuals profiling.	Monitoring shopping and shopping tendencies (e.g. alcohol, sweets).
3. Systematic monitoring of publicly accessible areas on a large scale <u>using elements of recognition of characteristics or properties of objects, which are present in the monitored area.</u> This group of systems <u>does not include</u> video surveillance systems, in which image is recorded and used only in case of the need for analysis of incidents of breach of law.	The means of public transport, the cities offering bicycles and car rental systems, setting paid parking zones.	Monitoring persons using services in public space, with the use of data going beyond the data necessary for service provision.
	Workplaces (monitoring of IT systems of e-mail, used software, access cards, etc.).	Systems for monitoring of working time and information flow in the tools used by employees (e.g. e-mail, Internet). Criteria : systematic monitoring (*vide* WP249[1]) + vulnerable data subjects.
	Processing of information obtained via the Internet of things (medical bands, smartwatches, etc.) and their transmission in the network using mobile devices such as a smartphone or tablet.	Collection and use of data by applications installed in mobile devices, including devices integrated with uniforms, helmets or otherwise connected with the person gathering data.
	Machine-to-Machine communication systems, in which the car informs its surrounding about its behaviour (movement) and in case of occurring risk receives from this surrounding (road infrastructure, other cars) warning messages.	Vehicles monitoring systems connecting to their surroundings, including other vehicles.

[1] Opinion 2/2017 on data processing at work (08.06.2017)

	Opinion of the European Economic and Social Committee on 'Radio Frequency Identification (RFID) (2007/C 256/13).	Systems using RFID in case where tags/labels are or can be attributed to individuals.
	Hospitals/Organizations conducting clinical research. Fitness clubs/entities/organisations collecting genetic material for research.	Patients/customers health data.
4. **Processing of <u>special categories of personal data and personal data relating to criminal convictions and offences</u> (sensitive data in the opinion of WP 29)**	Political parties, electoral committees, referendum committees and legislative initiatives, social organisations, election campaigns.	Processing of personal data concerning party membership and/or voting preferences by public or private authorities.
	Telecommunications operators; providers of utility services (electricity, gas, water) as regards smart metering – Recommendation 2012/148/EU by the European Commission of March 2012 on preparations for the roll-out of smart metering systems.	Regular measurement data processing allowing for observation of lifestyle, movement, intensity of the use of utility services, energy, etc. (e.g. geolocation data, data on used energy from smart meters, billing data concerning electronic communications, etc.).
	E-mail services; sporting achievements monitoring systems cooperating with fitness bands, using a cloud; applications provided by producers of electronic readers for purchasing books, electronic newspapers with noting functionalities, etc.	Websites and other IT systems offered to individuals for processing of information covering personal or household activities (for example cloud computing services for personal documents management, e-mail services, calendars, e-readers with notes taking function and various „life-logging" applications, which may contain very personal information), the disclosure or processing of which for the purposes other than household activities can be considered as very interfering in privacy.
5. Processing of biometric data <u>for the purpose of uniquely identifying a</u>	Facial recognition systems, identity verification in the workplace for the purpose of access control, identity verification in devices/applications (including	Entries to particular areas, premises or gaining access to specific account in the IT system for the purpose of e.g.

natural person or verifying access control	voice/fingerprint/facial recognition); systems for monitoring entries into particular premises; systems for settlement and record of banking, trading and insurance operations; systems for monitoring of entries to fitness clubs, hotels, etc.	executing a transaction order in the ICTS system or cash withdrawal from the ATM, etc.
6. Processing of genetic data	Laboratories/companies/hospitals offering genetic diagnostics	Medical diagnosis DNA tests Medical research
7. **Data processed on a large scale, where the notion of large scale concerns:** • **the number of persons whose data are processed,** • **the scope of processing,** • **the data storage period and** • **the geographical scope of processing**	Central system of: - educational information; - higher education information; - motor insurance services; - professional qualifications etc.	Central data filing systems supporting managing a particular group of persons for the purposes connected with the performance of public tasks, from which the data are made available in various scope, depending on their role and tasks related to the execution of these obligations.
	Social networks, Internet browsers, cable television service providers, subscription services with movies and TV programs available on devices with Internet connectivity	Collecting broad scope of data on websites viewed, shopping history, watched TV and radio programmes, etc.
8. Making comparisons, evaluating or drawing conclusions based on analysis of data obtained from various sources	Marketing companies that collect data from various sources, where there is data about clients, for the purpose of conducting targeted marketing campaigns for specific groups of customers.	Combining data from various state and/or public records.
	Marketing companies for the purpose of improving and expanding the profiles of potential clients and improving advertising services targeted at specific social groups;	Creating user profiles from filling systems from different sources (combining filling systems).

	companies supporting loyalty programs (shopping communities).	
	Social networks, retail chains, marketing companies, banks and financial institutions.	Collecting data on the websites viewed, banking operations, shopping in online stores and their subsequent analysis in order to create a profile of the person.
9. Processing of data concerning persons, whose evaluation and the services provided to them depend on the entities or persons, which have supervisory and/or evaluating powers	Services offering job, which adapt the offers to specific preferences of employers.	Processing of data, where classification or evaluation of data subjects e.g. in terms of age, sex, is made, and then this classification is used for presenting offers or other activities, which may affect the rights and freedoms of individuals, whose data are processed.
	Systems used for reporting irregularities (whistleblowing).	Systems used for reporting irregularities (e.g. related to corruption, mobbing) – in particular, where employees' data are processed in them.
10. Innovative use or application of technological or organisational solutions	Utility services sellers and distributors (electricity, gas, water, telecommunications services) implementing smart meters.	Remote metering systems, which - taking into account the scope and frequency of data collection – enable profiling of persons or groups of persons.
	Websites (services) processing data from devices such as Internet of Things, e.g. cameras equipped with localisation functions (GPS).	Systems for analysing and processing of data contained in metadata, e.g. photographs accompanied by geolocation data.
	Applying communication between devices (Internet of Things – e.g. beacons, drones) in public space and locations of public use.	Systems used for analysis and transfer of data to services providers with the use of mobile applications from wearable portable devices such as: smartwatches, smart bands, beacons, etc., analysing and transferring data to providers with the use of mobile applications.

	Applications with communication functions and software enabling exchange of information with immediate neighbourhood as well as remotely through telecommunications network.	Applying devices equipped in various types of interfaces (loudspeaker, microphone, camera) and software and communications system enabling transfer of data through telecommunications networks.
	Interactive toys.	Services and toys for children.
	Specialised advice and medical consultations, clinical research on an international scale.	Telemedicine consultations with centres outside the EU, transfer of medical personal data on an international scale.
11. In case where the processing itself „prevents data subjects from exercising a right or using a service or a contract"	Entities providing loans or credits and offering instalment sales.	Making credit decisions for potential clients based on information available in databases containing information about debtors or similar databases.
	Online stores and providers of other services such as games, music, lotteries, etc.	Making service usability dependent on income information, the amount of monthly expenses and other values obtained as a result of profiling
12. Processing of location data	IoT devices, applications and platforms. Data processing in the context of home and remote working. Processing location data of employees.	Processing which involves tracking of an individual's location (including communications networks and communications services, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service).