DPIA need assessment

Process name

Description of processing:

Evaluated processes

RISK LEVEL	**TRACKING AND MONITORING OF MOVEMENT AND BEHAVIOUR**
1 - high risk	Deliberate and continuous tracking of the movement or behavior of identified individuals or clearly defined groups of people that can be localized/idenitified in order to evaluate or further process the acquired data (eg. GPS position of employees).
2 - medium risk	Tracking of the movement or behavior of random, previously unknown or unidentified people concerning public space or publicly available online environment (e.g., monitoring a building's space) where individuals can be subsequently identified
3 - low risk	Tracking of the movement or behavior of random, previously unknown or unidentified people without interfering with the public space (eg direct monitoring of property, building)
4 - no risk	No tracking or monitoring

Choose the risk

Comments:

		DO NOT EDIT THE CELLS BELOW
High-risk factors (sum)		**0**
Medium-risk factors (sum)		**0**
Low-risk factors (sum)		**0**
DPIA to be carried out		DPIA not mandatory
DECISION		***<TO BE FILLED>***

INTRODUCTION
Below you can find categories of risky operations that shall be taken into account when assessing t
Protection Impact Assessment. Please specify the risk for each of those criteria for the process that

SPECIAL CATEGORIES OF DATA	VULNERABILITY OF SUBJECTS
Critical data processing - special categories of data according to Article 9 GDPR, information on criminal matters, financial data, personal communications or other expressions of a purely personal nature (private videos, etc.)	Group members defined by nationality, religion, sexual orientation, physical or mental disability, criminal conviction, etc.
Significant data - login data including passwords, data enabling the takeover or abuse of identity (name, date of birth, permanent address, signature, copies of ID documents, contact details, customer number, contract number, etc.), unique identifiers (personal identification number, social security number etc.), history of purchases, browsing history, or other behavioral or personal aspects that can lead to profile creation	Limited vulnerability: - time-limited or situation-limited groups such as migrants, sick, elderly, children, adolescents, applicants for welfare / benefits, employees, buyers of specific or sensitive services (eg drugs, sex toys), etc.
N/A	N/A
Common Data - identification, contact, social, property and economic (if they themselves cannot lead to identity abuse), work-related info, simple photos or records	No special characteristics

the need for conducting the Data
t is subject to the assessment.

LARGE SCALE PROCESSING	INVISIBLE PROCESSING
Processing at international or global level, large number of people (usually > 100k people), large data processing (deep profiles), systematic data collection from a large area or online environment	Processing that the person in question is not informed in advance and which he cannot practically influence, in particular, cannot exercise or may only partially exercise his rights.
State-level processing, medium number of people (<100k people), medium range of data (without creating profiles etc.)	Processing that the data subject can influence only partially, such as automated decision-making, processing for the purpose of the protection of rights of the controller or third parties, such as fraud investigation, assessment of personal aspects through registers, social networks, other publicly available resources that lead to decisions with substantial consequences
Local processing, low number of people (<10k persons), basic data	N/A
Small-scale local processing (<5k people)	The data subject is informed and can exercise his rights without any problems

PUBLICATION OF DATA	NEW TECHNOLOGIES, TECHNOLOGICALLY COMPLEX PROCESSING AND INNOVATIONS
Processing that leads to the publication of individuals' data that have not yet been published or publicly available	Processing using completely new technologies with which the controller has no experience (eg automated decision making, use of biometric data, genetic data, IoT, telematic services, artificial intelligence, big data analysis, etc.)
Disclosure of data that has not yet been disclosed or make public to a limited number of people	Processing using new technologies with which the controller has no experience but can obtain them from processors or other controllers, or there is sufficient documentation
Disclosure of data that has already been publicly available but has been processed in a new way or from which additional data have been derived	N/A
Data is not made public or disclosed to other entities	Standard solution, box solution, controller has experience

AUTOMATED DECISION-MAKING, PROFILING, DATA MATCHING

Processing includes automated individual decision-making, profiling leading to decisions with substantial consequences, scoring, behavioral or marketing profiling based on online tracking, social networks profiles etc.

Processing involves combining, merging or aggregating data from different sources and colected for different purposes without solely automated processing and without significant consequences for the data subject

Simple chain of operations or operations with variable or multiple relations

Data is not merged or aggregated from different sources

RELATIONSHIP WITH OTHER CONTROLLERS OR RECIPIENTS		
The range of other data controllers or recipients cannot be fully controlled.		
N/A		
The range of other data controllers or recipients can be controlled.		
N/A		

List of processing operations that require a DPIA

Categories of operations

Innovative technology

Processing involving the use of new technologies, or the novel application of existing technologies (including AI). Innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you, or use of existing technology in a new way

A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organizational solutions) when combined with any other criterion indicating high-risk operations (e.g. evaluation or scoring, or sensitive data).

Denial of service

Decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data.

Large-scale profiling

Any profiling of individuals on a large scale.

Biometric data

Any processing of biometric data for the purpose of uniquely identifying an individual.

A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion indicating high-risk operations.

Genetic data

Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.

A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion indicating high-risk operations.

Data matching

Combining, comparing or matching personal data obtained from multiple sources.

Invisible processing

‘Invisible processing’ occurs when you obtain personal data from somewhere other than directly from the individual themselves, and you don’t provide them with the privacy information required by Article 14 (providing information would prove impossible or involve disproportionate effort.

A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion indicating high-risk operations.

Tracking

Processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment.

A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion indicating high-risk operations.

Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services

The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.

Risk of physical harm

Where the processing is of such a nature that a personal data breach could jeopardize the [physical] health or safety of individuals.

Examples of particular projects requiring DPIA	Examples of particular projects requiring DPIA2
• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearables)	• Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) • Some IoT applications, depending on the specific circumstances of the processing
• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)	
• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring	• Social-media networks • Application of AI to existing process
• Facial recognition systems • Workplace access systems/identity verification	• Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)
• Medical diagnosis • DNA testing • Medical research	
• Fraud prevention • Direct marketing	• Monitoring personal use/uptake of statutory services or benefits • Federated identity assurance services
• List brokering • Direct marketing • Online tracking by third parties	• Online advertising • Data aggregation/data aggregation platforms • Re-use of publicly available data

• Social networks, software applications • Hardware/software offering fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation / data aggregation platforms	• Eye tracking • Data processing at the workplace • Data processing in the context of home and remote working • Processing location data of employees • Loyalty schemes • Tracing services (tele-matching, tele-appending) • Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing
• Connected toys • Social networks	
• Whistleblowing/complaint procedures • Social care records	