Data privacy impact assessment

moveUP

This document is the summary of the 25 pages original DPIA document. This shorter version was created to give an understandable overview of residual risks of processing health data and share the actions that moveUP is performing to safeguard your data.

1. Introduction

moveUP is a new technology that processes systematically identifiable personal and sensitive data on large scale and this data can be shared with different healthcare practioners (interoperability).

Large scale
• Number of patients, already more than 1200 patients • Amount of datapoints per patient > 400 • Retention time of medical data = 30 years • Large geographic area = BE, NL, FR, GER • Monitoring daily & periodically (medical scores)

Therefore, moveUP is obliged to perform a data processing impact assessment **(Art. 35).** Performing a risk analysis is not a new given, because this is one of the key actions of the quality management system of a medical device manufacturer such as moveUP.

2. Scope

The Product: The use of moveUP (App, patient website, dashboard webinterface, wearable) . All options (Prom, Companion, Coach, Therapy).
The Organizations activities, data processes (see point 4), including its subcontractors (see point 6).

3. Competences

moveUP invested in having the correct competences (in-house or outsourced) to help with our compliance strategy and to fully understand the requirements of the GDPR. Having these experts' judgements and advices contributes to identifying non-conformities, gaps and priorities. As part of our quality management system the need for extra training of every employee and the quality of service of the subcontractor are yearly reviewed.

Competences on board		
DPO	CISO	ADJUNCTS DPO / CISO
INTERNAL IT SECURITY AUDITOR	EXTERNAL IT SECURITY AUDITOR	SOFTWARE TEAM WITH IT SECURITY KNOWLEDGE

The credentials of our designated DPO (**Art.37)** are the following:
Name: Saba Parsa **; Contact:** sp@altalaw.be **; Background**: Lawyer & DPO certified

4. Data processes

Determining the organizations data processing activities, nature of processing and which categories of data that are collected are crucial elements for risk evaluation.

4.1. Processes

Processing activity	Controllers	Purposes	Transfer outside the European Economic Area*	Sensitive Data
Managing patient data, via system, EHR, GP, or via the surgeon, and using them to adapt the treatment (patient or no-patient involvement)	b.clinic or care institution or hospital	Personalized Rehabilitation after joint replacement / surgery Providing personalized treatment to reach the best health outcome	NO*	**YES**
First collection of patient's data who are candidates for the system, necessary to prepare onboarding, not yet started	b.clinic or care institution or hospital	Start preparations for follow-up, also for best fit option (companion, coach, therapy)	NO*	**YES, but limited** (surgery date, type of surgery…)
PROM collection after rehabilitation	b.clinic or care institution or hospital	Long-term follow-up of health state patient / pathology / rehabilitation / intervention	NO*	**YES**
Gathering patient data during onboarding / registration necessary to sign the contract.	moveUP	Subscription – signing contract	NO*	NO
Data processing of HCP's data, to access the moveUP dashboard to follow-up patients, sharing patient data / data transfer / portability	moveUP	rehabilitation, healthcare management	NO*	NO
Using pseudomized patient data for general protocol improvement (profiling, learn from mistakes, etc..)	moveUP	Obligations medical device	NO	NO
Legal obligation of processing employee data, accounting, notary	moveUP	HR- and business management company obligations	NO	**YES**
Collecting important feedback, adverse event, complaints in JIRA tool	moveUP	Post-market surveillance & client support : Obligations medical device	NO	**YES**
Process data for product, service, research (such as	moveUP	Obligations medical device	NO*	NO

user design/experience interviews, satisfaction surveys, ...)				

* Our DPO opinion: On July 16th 2020 the EU-US privacy shield has been invalidated by the European Union Court of Justice. Since then data transfers to the united states are prohibited. Furthermore, the Court also invalided the use of the Standard Contractual Clauses Commission, for the data transfer to US. But in our case, I would like to remind that:
A third country transfer under the GDPR concerns flows of personal data to and from countries outside the Union and international organizations. In any event, transfers to third countries and international organizations may only be carried out in full compliance with this Regulation.

4.2. Personal and Sensitive data – Categories

	Patient	HCP	Hospital
Contact data = personal data	✓	✓	✓
Invoice data=personal data	✓	✓	✓
Marketing data = personal data	✓	✓	✓
Medical data = Sensitive data	✓	✓	✓
Data about usage of moveUP and its services = personal data		✓	✓
Financial data = personal data		✓	✓
Salary data = personal data		✓	✓

COMMUNICATION BETWEEN PATIENT AND HCP (chat function)

The content of the chat messages between patient and healthcare provider is also saved. This storage is a form of processing and therefore falls under the GDPR legislation. The content of this chat may contain other information (categories) than the information mentioned above. For example, a patient can share personal experiences that have nothing to do with the rehabilitation itself.

4.3. Nature of processing

- Collection (e.g. prom, quesitonnaires, objective stepdata , mails, complaints)
- Recording (e.g. video analysis joint, recording consent)
- Storage (e.g. medical records, sendgrid list of mailadresses)
- Comparison (e.g. health status compared to other knee patients boxplot)
- Erasure / destruction (e.g. right to be forgotten, unsubscribe from mail)
- Communication (e.g. chat, onepager shared)
- Adaptation / alteration (e.g. accurate / correct data)
- Retrieval (e.g. onepager, datamodel)
- Disclosure by transfer (e.g. onepager to surgeon, in-house share for technical support)

- Structuring / organization (e.g. category mails, database ordening, rules and permissions to prevent unauthorized acces)
- Aggregation (e.g. datamodel, research)

5. Legal grounds for this processing?

moveUP has determined for each data processing activity the legal ground and if there is a consent needed or not.

Processing activity	Legal ground	Consent needed yes or no?
Managing patient data, via system, EHR, GP, or via the surgeon, and using them to adapt the treatment (patient or no-patient involvement)	Article 6 §1 c) and art. 9 §2 f), 9 §3 And for the transfer to HCP : Article 6 §1 a) and art. 9 § 2 a) and f), 9 §3	☐ I agree with the moveUP privacy policy. I'm aware that doctors and healthcare practitioners who use moveUP will process my data in function of my follow-up a/o treatment. **(This checkbox is mandatory to be selected to be able to start with moveUP**) ☐ I give my consent to the transfer to my heath care provider **(This checkbox is mandatory to be selected to be able to share data with HCP**)
First collection of patient's data who are candidates for the system, necessary to prepare onboarding, not yet started		
PROM collection after rehabilitation		
Data processing of HCP's data, to access the moveUP dashboard to follow-up patients, sharing patient data / data transfer / portability		
Using pseudomized patient data for general protocol improvement (profiling, learn from mistakes, etc..).		
Legal obligation of processing employee data, accounting, notary	Article 6 §1 c) and art. 9 §2 b), 9 §3	No consent needed, because mandatory by law.
Data processing technical support	Article 6 §1 c) and art. 9 §2 f) And it is also necessary for the performance of a contract	No consent needed, because mandatory by law.
Collecting important feedback, adverse event, complaints in JIRA tool	Article 6 §1 c) and art. 9 §2 f)) necessary to be compliant to medical device regulation	No consent needed, because mandatory by law.
Process data for product, service, purposes (such as user design/experience interviews, satisfaction surveys, clinical evaluation,...)	Art. 6 §1 a) and art. 9 §2 a) consent	☐ Consent should be asked during registration (separate checkbox)
Process data for research purposes (such as user design/experience interviews,	Art. 6 §1 f) and art. 9 §2 j) necessary to be compliant to medical device regulation	Opt-out system Interest have been assessed and anonymization and

satisfaction surveys, clinical evaluation,...)		pseudonymization of data are done when is possible.
Gathering personal data during for registration **necessary to sign the contract**. Patients / HCP / Partners	Art. 6 §1 b) necessary for the performance of a contract	No consent needed, this data is necessary to start the moveUP service. (contract B2B / B2C relationship)

6. Subcontractors

There is a strict selection of subcontractors, because of the increased risks (cloud, accessible on a distance, sensitive data, confidential data (IP), ...). moveUP has an Approved Supplier List process, which means that the subcontractors are selected conform predefined criteria (e.g. security certifications) and yearly reviewed (contracts / quality of service / performance).

Processing activity	Location
Customer support for feedback, complaint handling	EU
Software development company	EU
Document management , productivity tools and e-mails	EU
Providers of mailing solutions.	EU
Document management	EU
Database infrastructure and service provider	EU
Database management systeem	EU
Providers of IT solutions and maintenance of the website.	EU
CRM	EU
Social media	EU
Cloudprovider and database server	EU
Lawyer(s) and legal services provider(s)	EU

HR services and social security	EU
Accountants and financial services providers: Invoicing and payment.	EU
Communication tools.	EU
Banks	EU

7. Basic Principles

7.1. Lawfulness

As processor we are not allowed to define the purposes and by extension the legal ground of the processing. The legal ground we describe here are our customer legal ground under GDPR.
Furthermore, moveUP processes for its customers the sensitive data, which is allowed by the provision 9 §2 f) of the GDPR . In effect, moveUP is a structural part of the patient's follow-up and/or treatment with the aim to visualize and improve the patient's health. For this reason, it is appropriate to have a contractual agreement between moveUP and patient and moveUP and hospital, but it does not change our role, as processor, in the processing or the lawfulness of the processing. We also provide a privacy policy to our customers to explain the legal ground.

As controller, we verify that the purposes of our processing are defined, precise and explicit (in our register, in our privacy policies, ...). Then, for each purpose pursuant to Article 6, we determine a legal basis for processing. When we process sensitive data, we verify that one of the conditions of article 9 is also met.
Finally, we verify that the data used is necessary for the processing, relevant, updated and we communicate to the data subjects.

7.2. Information and transparency

Via an introduction text and extensive privacy policy, which is retrievable during registration, on the website, in the app, we inform end users about the who, what, when, how,etc…
Contact details are multiple times shared, so the end user is able to reach us when more information is needed / wanted. An important update of the privacy policy is notified to the end user: pop-up in the app with the new privacy policy.
With the DPA and DPIA also top management of care centers / hospitals are informed by the product moveUP, it's (gdpr) role and remaining risks.

7.3. Clear purpose

The purpose of moveUP processing (as controller) is made clear to the HCP via extensive e-learning modules.
The different purposes, are described in the privacy policy (statistical, medical purposes, legitimate interest)
As processor, we do not define the purposes of our controller, but we communicate them to the data subject.

7.4. Data minimization

Data are processed because of the necessity for providing the moveUP Service (follow-up and rehab of patients) . We only process data that is necessary for our and our controllers purposes. We process sufficient data to fulfill those purposes. In table below an example of necessity:

Actor	Category	Element	Necessity
Patient	Identification data	Name and first name	Patientidentification
		Birthdata	
		Social secretary	
		Contact number	
		Gender	
		E-mail	Login moveUP
		Password	
		Home adress	Invoicing Service providing Result analyses
		Marital status	
	Healthdata (pre-operative)	Medical profile: BMI, comorbiditits, smoke/non-smoker, previous operations	Creating patient profile
		Social profile	Service providing Result analysis
		Medication	Personal rehabilitation
	Healthdata (During operation)	Type intervention + date	Personal rehabliation and correct followup
		Name surgeon + riziv number	Correct followup & data privacy (therapeutical link)
		Type implant	Personal rehabilitation and correct followup
		Type anesthesic	
		Duration of operation	
	Healthdata (during hosptial stay)	Length of stay	Health state and economic insight
		Criteria for discharge	
		Medication intake	
	Healthdata (rehabilitation & follow-up)	Physical activity wearable	Personal rehabliation and correct followup
		Sleep data wearable	
		Photo's joint / wound	
		Video's gait analysis / rom	
		PROM data	
		Pain level and intensity	
		Mobility (dailty activities, sportive acitivities, general wellbeing)	
	Admin data	Payment data	Not to be filled out when invoicing goes via hospital
		Fragmented payment decision	
		Mutuality sticker	
		RIZIV number	
		Facturation adress	
HCP (e.g. physio)	Administrative identification data	Name, First name, Social security number	Identification HCP(ehealth)

		E-mail Password	Login platform

7.5. Accurate

Identification data (patient)

- Anyone with a personal account can manage and modify his / her account information
- After registration, the patient can no longer make any adjustments to his profile. The adjustments are always made via the care provider, at the request of the patient (via chat, e-mail, telephone, ...)

Health data
The patient is informed that it is important to answer the questionnaires as much as possible and correctly.
The data from the activity tracker is accurately read, collected and managed if:

- The wearable is properly installed (eg has set the correct time zone and date)
- The wearable is used properly (eg patient does not share the wearable with other persons)

Administrative identification data (healthcare provider)

- Data can only be changed through the intervention of the admin account
- The administrator role can edit and delete account details of healthcare providers

7.6. Minimum retention time

Dataprocessing	Time
Management health data	Maintained for 30 years after the contractual relationship has ended, with regard to a correct, complete and current medical record
Management healthdata in the context of a clinical study	Are kept for 20 years after the end of the study
Accounting data related to the moveUP subscription	will be kept for 10 years, in accordance with the 10-year statute of limitations for this claim
Other data	will be kept for a period necessary to fulfill our legitimate interest, as the risk of a data breach does not outweigh your human rights. For example, the profiles are kept for 2 years
In the event of a dispute	Will potentially be held longer than the deadlines stated above for legal defense. In this case, the retention of relevant data can be extended to the level necessary in function of the dispute and to the closure of the dispute.

7.7. Data integrity & confidentiality

The therapeutic relationship and professional secrecy apply. To preserve confidentiality only

(third party) healthcare providers with a justified (therapeutic) relationship with the patient can access, adjust or receive data:

- In-hospital, such as
    - Orthopedic department secretary for onboarding & registration help
    - Surgeon
    - Physical therapist
    - Nurse
- (Virtual) care institutions, such as
    - B.clinic
- Out of hospital, such as
    - General practitioner
    - Physical therapist

7.8. User rights

All explained in the privacy policy and mentioned in the introduction text during registration.
Contact details shared (moveUP & moveUP's DPO) for more info about user rights or to excise a right.

7.8.1. Exercise a right

As stated in the moveUP privacy policy:We attach great importance to the rights that you have as a data subject. We are at your service and invite you to contact our contact person at the following email address: privacy@moveUP.care or via our generic contact address: info@moveUP.care or by post to our postal address. We have also proceeded to appoint a DPO, who is at your disposal at the following email address: sp@altalaw.be.

7.8.2. Right of access

As stated in moveUP's privacy policy:
You can at any time request information about our treatments, the objectives pursued, the categories of personal data we hold about you, the categories of recipients of this data (third countries or international organizations), the retention periods or criteria for determining this deadlines, your other rights, other sources of your data and the existence of an automated decision-making process.

7.8.3. Right of data transfer

As stated in the moveUP privacy policy:
If your data is treated as part of our contractual obligations or after your consent, you have the right to have your personal data transferred in the form in which we keep it or to have it transferred to another designated controller by you.
To exercise this right, you must indicate this on the form that we make available on our website. You can also send us an email at the following address: privacy@moveUP.care.

7.8.4. Right of limitation

As stated in the moveUP privacy policy:
You have the right to request that the processing of your personal data be restricted when:
1. You dispute the accuracy of these data.

2. You are within the waiting period necessary to assess relevant interests before exercising the right to object to the processing of certain personal data.
3. The processing of your personal data is illegal, but you do not want to exercise your right to erasure.
4. We no longer need your personal data for the purposes set out in this data protection statement, but you need it in the context of legal action.

7.8.5. Right of objection

As stated in the moveUP privacy policy:
You can object to the processing of your personal data if your data is processed on the basis of our legitimate interests or on the basis of consent. To exercise this right, please send us an email at the following address: privacy@moveUP.care. You can also click on "unsubscribe" which you will find in every email you receive from us.

7.8.6. Right for erasure

In the cases provided for by the General Data Protection Regulation (GDPR) or the law, we will proceed with the deletion of your personal data at your request. In principle you can exercise your rights free of charge. You can also send us an email at the following address: privacy@moveUP.care.

We will inform you in writing of the action we have taken at your request no later than one month after receipt of your request. Depending on the difficulty of your request or the number of requests we receive from other people, this period can be extended by two months. In this case, we will notify you of this extension within one month of receiving your application. In some cases (eg legal obligations, rights of others, limitation periods, ...), you cannot exercise your rights, in whole or in part. You will then be informed as to why we cannot fully comply with your request.

7.8.7. Right for rectification

As stated in the moveUP privacy policy:
You can also request to correct or supplement your data if it turns out to be incorrect or incomplete. When you exercise this right, you must specify the exact data that you want to see corrected and supplemented. We will answer your question as soon as possible, however we are obliged to consider the rights and freedoms of others when providing this information.

7.8.8. Right of withdraw consent our object to processing based on legitimate interest

As stated in the moveUP privacy policy: You can withdraw your consent anytime by contacting us (privacy@moveup.care).

7.8.9. Right of information

Each patient of moveUP account has agreed to the terms of use and privacy policy of moveUP when creating the account. These provide, among other things, more information about the processing that is done by moveUP. Even when logged in, the document remains available so that the patient can always consult it when necessary. For HCP this module is lacking.

Each enduser can at any time request information about our dataprocesses, the objectives pursued, the categories of personal data we hold about you, the categories of recipients of this

data (third countries or international organizations), the retention periods or criteria for determining this deadlines, your other rights, other sources of your data and the existence of an automated decision-making process. We have an extensive privacy policy.

8. Risks and measures

Risks related to data privacy and IT security are analysed and are part of the risk management (ISO 14791) of the medical device product and organisation since 2017. With this risk-based mindset moveUP has already put a lot of measures in place in the context of information security (also stated in the privacy policy):

- Security and encryption
- Security of servers through certification
- Organization of awareness sessions and implementation of an internal IT security policy
- Shield entrances as much as possible
- Pseudonymization and anonymization of data
- Detailed procedure for data leaks

….

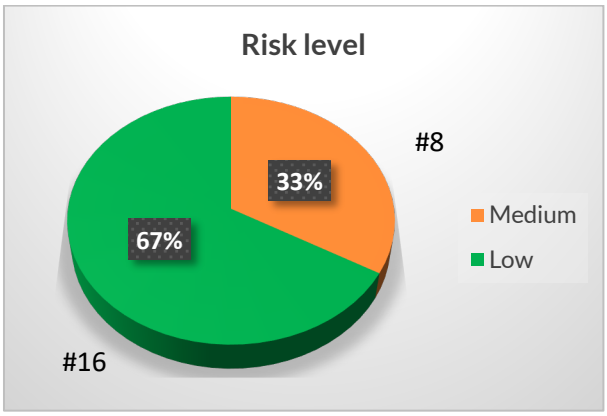
For further improvements the previous IT security roadmap included to be ISO 27001 certified. The certification for ISO 27001 was received in June 2020, but safeguarding data privacy and performing risk management is a continues action throughout the lifecycle of our product and organisation activities. That's why an in-depth version of the DPIA was performed in August 2020.

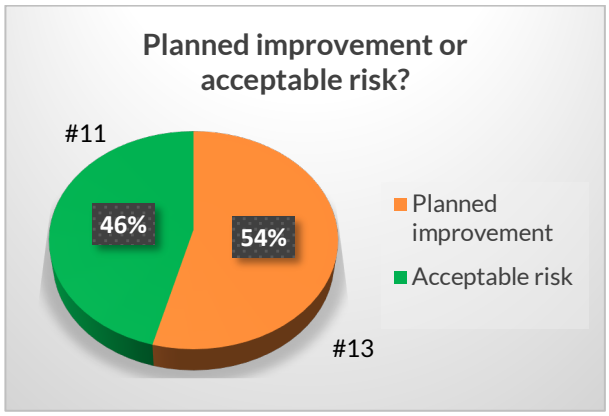
To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. Also, we looked to the information safety table for the correct estimation of the impact.

Impact category	Information safety		
Subcategory / score	Integrity	Confidentiality	Availability
	Infringement of the integrity of company information or personal data.	Violation of confidentiality due to the leakage of confidential business information. Infringement of confidentiality due to the leakage of personal data of citizens.	Company information is not available. Citizen data is not available.
1-LOW	Public information has been compromised. The personal data of one or only a few individuals has been compromised.	Public information is disclosed. The personal data of one or only a few individuals has been disclosed.	Public information is not available. The personal data of one or only a few individuals is not available.
2	Standard business data has been compromised (accounting,…). Multiple individuals' personal data has been compromised.	Standard company data is made available (accounting,…). The personal data of several individuals has been disclosed.	Standard company data is not available (accounting,…). The personal data of several individuals is not available.
3-MEDIUM	Sensitive business information has been compromised (HR data, ..).The sensitive data of one or more persons or the personal data of a population group have been compromised.	Sensitive business information is disclosed (HR data, ..). The sensitive data of one or more persons or the personal data of a population group have been disclosed.	Sensitive company information is not available (HR data, ..). The sensitive data of one or a few persons or the personal data of a population group are not available

4	Very sensitive business information has been compromised (entire business processes). The sensitive data of a population group or the personal data of several population groups has been compromised.	Very sensitive business information is disclosed (entire business processes). The sensitive data of a population group or the personal data of several population groups has been disclosed	Very sensitive business information is not available (entire business processes). The sensitive data of a population group or the personal data of several population groups is not available.
5-HIGH	Business-critical information has been compromised. The sensitive data of several population groups or the personal data of the entire population has been compromised.	Business-critical information is disclosed. The sensitive data of several population groups or the personal data of the entire population has been disclosed.	Business critical information is not available. The sensitive data of several population groups or the personal data of the entire population is not available.

After profound, detailed and critical thinking, we defined 24 remaining risks. We described the problems and (possible) improvements extensively. Based on this risk analysis we can conclude that we don't need to inform the ICO (no high risks identified), but we identified that for 13 risks an improvement is necessary. No urgent immediate corrections to be done, but we wish to mitigate the medium risks as fast as possible.





Some examples of planned improvements that are top priority:

- No identifiable dataset in MySQL (resolved in October 2020).
- Implement a general two factor authentication, next to 'itsme' which is already operational.
- Sign off DPA's with all the hospitals where moveUP is/will be used. Every hospital has his own interpretation of the controller-processor role and the workload for the legal departments (on hospital and our side) leaded to delays in finalizing the DPA.
- Improving the password policy for end-users (using the moveUP product) and employees (working in the moveUP organization).
- Digitalize the acceptance of Terms and Conditions and Privacy policy for HCP (dashboard side). On patient side this is already operational.
- Some DPA contracts missing for our processors or DPA's lacking IT security requirements. However, there is a strict selection (gdpr compliance / security certificates required) and yearly evaluation of the processors we choose.

moveUP has established a new IT security roadmap, including the proposed corrections explained above. The full IT security roadmap is based on the results of:

1. Internal Audit ISO 27001
2. External Audit ISO 27001
3. Feedback DPO / hospitals
4. Risk analysis ISO 14791
5. DPIA
6. Assessment Annex III zorgicuronet template: Questionnaire on information security and data protection
7. Stakeholders / third party / potential partners feedback

To keep improving and go deeper in the DPIA, we are engaged in a platform smart-gdpr. ''Smart Global Privacy® provides a comprehensive toolset for the entire team (Managers, Project Leaders, Data Protection Officers and/or Consultants) to profoundly minimize the effort, cost, delay and risk of GDPR compliance''.

moveUP will re-do the DPIA on a yearly basis and evaluate if the measures were implemented and if risks can be mitigated further. Intermediate discussing about the progress are part of the management review meetings.

9. Acknowledgement

With this document we want to show the efforts for compliance with **Art. 35** of the GDPR. Extra checklist added below.

Art. 35 paragaph	Are we compliant? Yes, No or N/A
1.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.	Yes, see this full document. Risk management product and organisational level also retrievable in Matrix Requirements.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	Yes, new version of DPIA is reviewed in the week of 1/09/2020.
A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (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; => Dossier: Automated Decision In Individual Cases, Profiling (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 referred to in Article 10; or => Dossier: Extensive Processing (c) a systematic monitoring of a publicly accessible area on a large scale. => Dossier: Extensive Processing	Yes, see point 4, 7 and 8.
The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact	N/A

assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.	
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.	N/A
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	N/A
The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; => Dossier: Legitimate Interests (Controller) (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and => Recital: 75 => Dossier: Risk For Rights And Freedoms (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Yes
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.	N/A
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.	Yes, feedback collected and analysed
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.	Yes, see point 5 legal grounds.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	Yes, GDPR topic to be discussed during management review meeting, which includes also review of risks and mitigations.