Data Protection Impact Assessment

WMW – Private Personal Proximity (Workplace distancing)

May 2020

CONTENT

1 INTRODUCTION

This Data Protection Impact Assessment (DPIA) was conducted by CLEAR DIGITAL for its data processing activities for the "private personal proximity" or "workplace distancing". This is a platform that is built to help employers to restart their business again and to make sure employees are safe and monitor if they can keep their distance. The scope of this DPIA is only for the WMW-HUB ppp-platform, where ppp means private personal proximity

1.1 What is private proximity registration?

The product of CLEAR DIGITAL protects the workforce of employers by warning for close encounters and tracing the 'contacts' the employees had on the work floor by giving them a dedicated hardware device (e.g. badge, watch).

1.2 What is a DPIA?

A DPIA is an instrument for the structured and standardised identification and assessment of the impact on data subjects of projects involving the processing of personal data. Based on this, measures are taken to prevent or reduce the impact on the data subjects.

1.3 Why does CLEAR DIGITAL perform this DPIA as a processor?

Although CLEAR DIGITAL is only a data processor for the intended purposes, it performs this DPIA to assess the data protection impact of a technology product because the product is likely to be used by different data controllers. Of course, the data controller deploying and implementing the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be by this DPIA prepared by the product provider. This is conform with the advise of the Working Party 29 on DPIAs: WP248_rev1.

CLEAR DIGITAL also performs this DPIA and keeps it up to date because it values data protection and wants to proof that the product is built with data protection by default and data protection by design (article 25 GDPR) in mind.

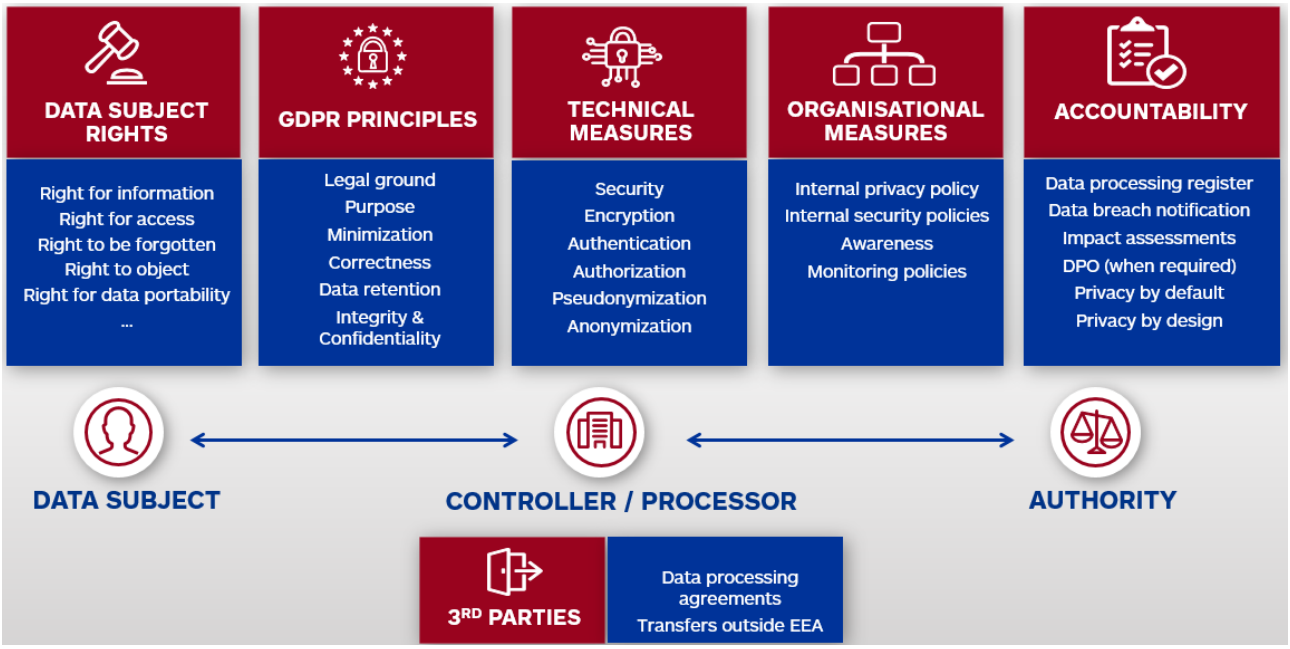
1.4 What approach is used to perform this DPIA?

The methodology used to conduct this DPIA is based on:

- the guidance contained in Article 35, Recital 75 and Recital 90 of the EU's General Data Protection Regulation (GDPR);
- the WP29 Guidelines on DPIAs: WP248_rev1 ;
- the UK Information Commissioner's Office (ICO) website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/;
- The DPIA template of the ICO: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
- CNIL's Privacy Impact Assessment Methodology: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf;
- risk assessment concepts from the CNIL's Methodology for Privacy Risk Management: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

To identify risks, we will run over the 6 domains (as explained in the figure below):

- Data subject rights
- GDPR principles
- Accountability
- Technical measures
- Organisational measures
- 3rd parties



External privacy experts (Privatum) and data security specialists were also consulted in the development of this DPIA.

To asses the risk and necessary measures this DPIA also takes into account specific guidelines set by privacy authorities related to contact tracing:

- Advise of the CNIL for employers on processing personal data of their employees related to Covid-19 : https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles-par-les
- ICO contact tracing recommendations: https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf
- EDPB contact tracing guidelines: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
- European E-Health toolbox: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

2 GLOSSARY

- CNIL: The data protection authority of France
- EDPB: The European Data Protection Board
- ICO: The data protection authority of the UK
- On premise: The installation of the ppp-platform is done on a server or data center that is under responsibility of the controller.
- SaaS: Software as a service. This means that CLEAR DIGITAL is responsible for the hosting of the ppp-platform.
- WP29: The working party 29 which is the predecessor (before GDPR) of the EDPB

3 STEP 1: IDENTIFY THE NEED FOR A DPIA

Article 27 GDPR states that the Controller should perform a DPIA when "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*". In its advice WP248/01 on DPIAs the WP29 mentioned 9 criteria that should be considered to evaluate if there is a high risk. If the processing meets 2 of those 9 criteria, the Controller is required to do a DPIA.

3.1 Criteria for high risk processing

Mark the criteria that are applicable for the scope of this DPIA:

Criteria	Applicable	Reasoning
Evaluation or scoring	Yes	The behaviour of employees can possible be evaluated when there is reporting on the number of encounters that were too close. So there could be a ranking of "bad" employees.
Automated decision making with legal or similar significant effect	No	The product does not make automated decisions that has direct consequences to the employee.
Systematic monitoring	Yes	Employees will be observed during their job whether they keep a safe distance from their colleagues.
Sensitive date or data or data of highly personal nature	Yes	Who an employee encounters, even on the work floor is data of highly personal nature?
Data processed on a large scale	No	Depending on the number of employees of the controller. But by default, we consider that there is no large scale. For the processor CLEAR DIGITAL, however, if many controllers use the tool, there will be a large scale.
Matching or combining datasets	No	The product generates its own data and is not combining datasets. The controller however could be able to combine datasets, but this will be out of scope for this product and thus this DPIA.
Data concerning vulnerable data subjects	Yes	The data subject is an employee. The controller is the employer. There is a power imbalance between those two.
Innovative use or applying new technological or organisational solutions	Yes	Contact tracing and distancing are new concepts due to COVID-19.
Processing that prevents data subjects from exercising a right using a service or a contract	Yes	The tracing of close encounters might lead to the decision of an employer to ask an employee to not come to work anymore and stay at home because one of the colleagues that he/she worked with was diagnosed with COVID-19.

3.2 Conclusion

The controller is required to perform a DPIA, because more than 2 criteria are met when implementing private proximity registration.

Our conclusion is confirmed by the ICO in its contact tracing recommendations: "The ICO considers that a Data Protection Impact Assessment (DPIA) is required for contact tracing solutions prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of individuals.".

4 STEP 2: DESCRIBE THE PROCESSING

4.1 Describe the nature of the processing

4.1.1 How is data collected, used, stored and deleted?

Private Personal Proximity (PPP) is a low-level proximity registration solution that uses radio technology (BLE, UWB, …) to detect the distance and proximity of 2 wearable devices. Employees will receive a dedicated hardware device (e.g. badge, watch):

When a proximity is detected both devices will make a sound and vibrate, and they will send the other device's ID to a central server (that can be on premise or in the cloud). The data is not shared public and the solution is to be seen as a private network.

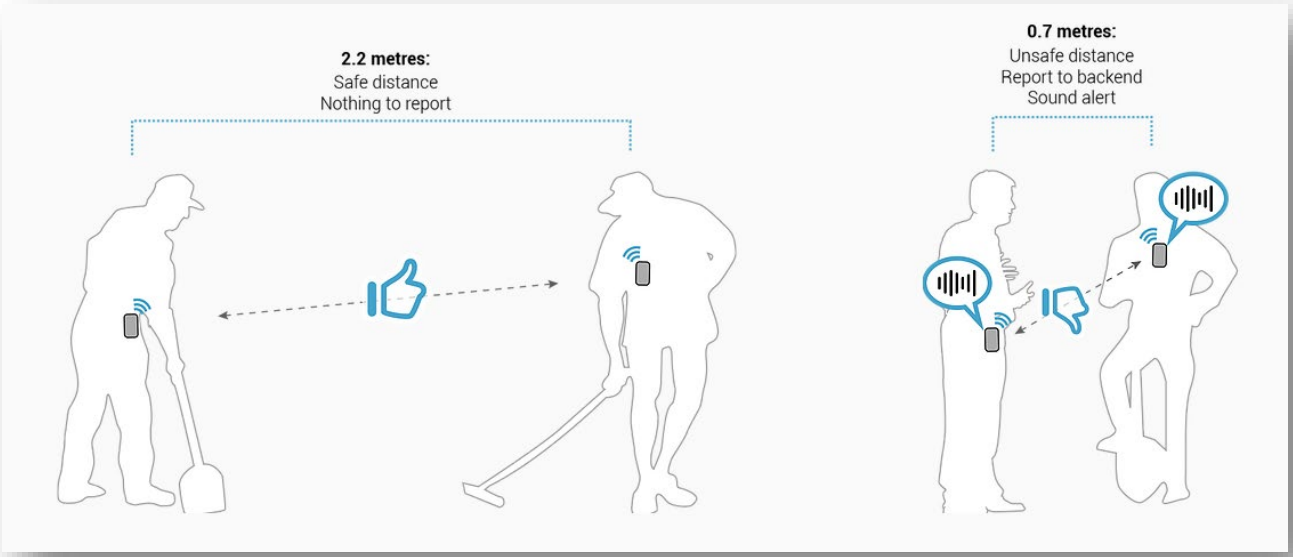
On the platform, the people wearing the device (=employee/visitor) are seen as “assets”. An asset can be registered on the platform and is identified by a unique ID. This ID is linked to a unique device identifier (the wearable).

The overall intention of the solution is to warn people when they are too close to each other (social distance) and to record every time that they have been too close for later possible retrieval. This means that no data is recorded when the applicable minimum distance is respected.

When a proximity is detected both devices will make a sound and vibrate, and they will send the following data to a central server (that can be installed on premise or in the cloud):

- Each other device's ID
- the duration of the close encounter
- the times of the close encounter

There is no information about the location (where in the company) of the proximity sent to the server.



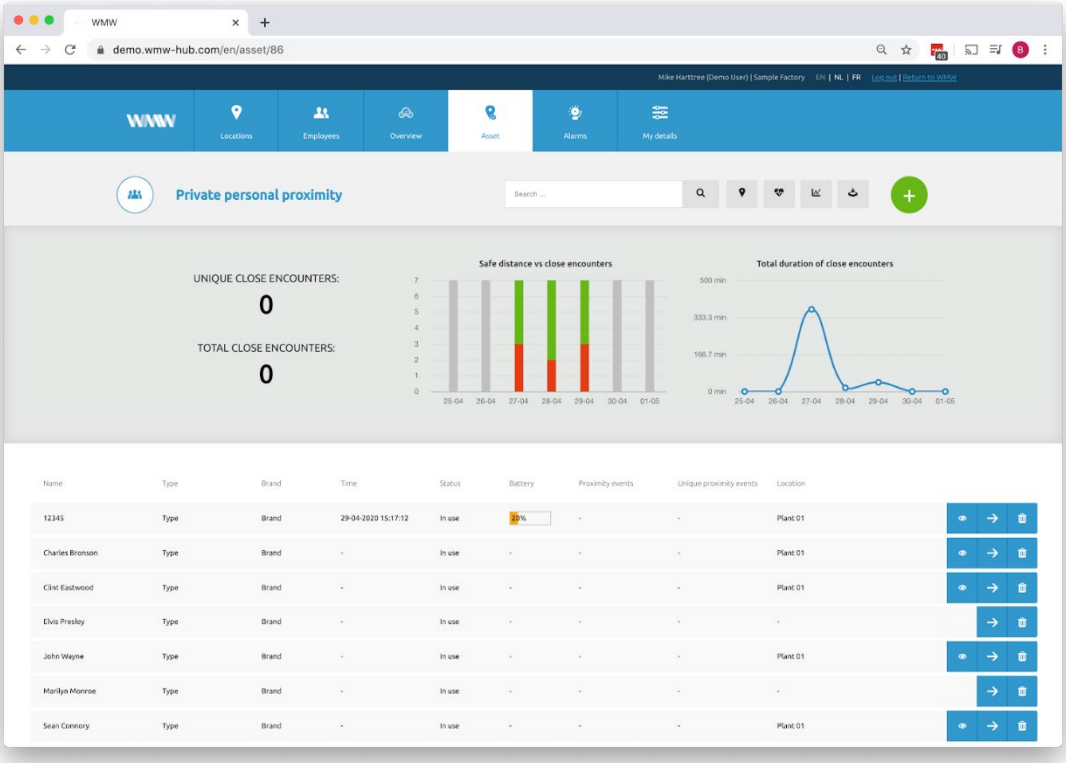
The platform doesn't collect proximities outside the company of the employer.

An admin on a platform can delete "assets".

The collected data will be used for two purposes. One the one hand the data will be used to check if social distancing is respected and on the other hand the data can be used for contact tracing.

1. **Social distancing**

The data will be used to monitor if the social distancing is respected. The monitoring will happen on two levels (general and specific monitoring).



a. <u>General monitoring</u>

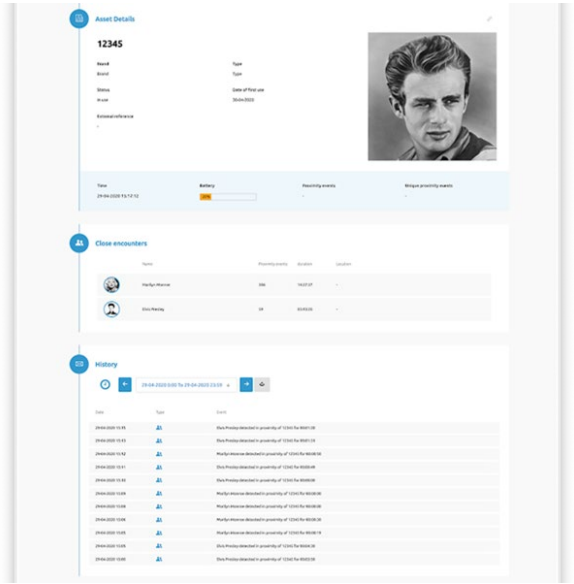
General monitoring is analysing the total close encounters on a floor, in a zone etc. without identifying a unique asset. This info will help customer to identify risks. For example, the data could identify that the taken measures are insufficient to respect the social distancing (e.g. a passage that is too narrow or too many employees that work on the same production line).

b. Specific monitoring

Specific monitoring is the analysis of the close encounters of a unique ID.

2. Contact tracing

When someone has been found ill, or forms a risk of being infected by the virus, the ID of that person is entered into the system. From this point on, the administrator can backtrack the ID's of other 'assets' that have been in his/her proximity over a set period of time.



4.1.2 What is the source of the data?

When two assets (employees) have an encounter that's too close, it triggers a report message to the central server.

The hardware devices also send battery status and an "alive message" at fixed intervals.

4.1.3 Will the data be shared with anyone?

The data can be seen by an administrator of the platform for an employer.

The data can be shared with the following parties:

- The close encounters of an employee can be given to the employee when he/she notifies the employer when he/she has diagnosed with COVID-19. And the employee can share the close encounters with a national contact tracing team.
- When diagnosed with COVID-19 the employee can tell the national contact tracing team to contact the company administrator of the employer, so that administrator might directly give the names of the people that had close encounters with the infected employee.

4.1.4 What types of processing identified as likely high risk are involved?

- See paragraph 3.1 of this DPIA

4.2 Describe the scope of the processing

4.2.1 What is the nature of the data?

The following data is captured on the platform:

- Asset (employee) identifier (required)
- Employer (customer)
- Department or location
- ID of the hardware device
- Proximity (device ID, other device ID, duration of the proximity, time of the proximity)
- Alive event of the hardware device
- Battery status of the hardware device

The collected data includes contact tracing, but only on the work floor. So, there is no contact tracing in the spare time or private atmosphere of the data subject.

Depending on the processes on how the product is used, medical data could be deducted. For instance if there is a log file on whose contacts where viewed or exported and there is an organisational process in place where an admin only views the proximity contacts of an employee when that employee indicates he/she is infected with COVID-19, those log files reflect that employee's medical condition.

4.2.2 How much data will be collected and used?

Only the close proximities will be collected and used. The employer can configure in the product what the definition is of a close proximity (how far). If everyone respects the social distancing on the work floor no data proximities are captured.

4.2.3 How often?

Every workday of the employee, but only the close encounters. Employees can turn off the hardware device.

4.2.4 How long will you keep it?

The personal data must only be processed for the duration of the COVID-19 crisis. Afterwards the data will be erased or anonymised. The purpose for the use of the anonymised data will be to maintain the statistics per department or location. So, lessons could be learned for the controller and measures can be taken to prepare for a next pandemic where social distancing is needed.

4.2.5 How many individuals are affected?

This is decided by the controller. There are a few options:

- All employees
- All employees of a certain department
- All employees of a certain location
- Only employees that belong to a risk group
- A mix of the above

4.2.6 What geographical area does it cover?

The monitoring of proximities is only done at the employer, in a certain fixed area on the work floor.

4.3 Describe the context of the processing

4.3.1 What is the nature of your relationship with the data subjects?

The data subject is an employee of the controller.

4.3.2 How much control will the data subject have?

A hardware device can be turned off by the data subject. When the employee leaves the company, the data of the employee can be deleted or anonymised.

4.3.3 Does the data subject expect that the controller will use the data in this way?

The solution of the contract tracing is made in such a way that the employee needs to receive a dedicated hardware device from the controller before the platform can register near encounters. This means that the controller needs to explain what the purpose of this new hardware device is. The situation would be different if the tracing was done with devices that the employees already use or carry with them, because that would give the controller the opportunity to capture the proximities secretly.

4.3.4 Are the data subjects' children or other vulnerable groups?

Within the PPP-platform anyone can be a data subject. So, if the controller for example is a school and gives a device to all of its students then the data subject can be a child. However, in a normal factory/company the employees will be over the age of 16 years.

The data subject (employee) is vulnerable in regard to the controller (employer) because of the power imbalance between the two.

4.3.5 Are there prior concerns over this type of processing or security flaws?

During the COVID-19 crisis there has been a public debate about privacy and contact tracing. It will require a good communication the controller implements this PPP platform only on the work floor and with the purpose to make it a safe workplace for all employees. It will also be important to mention that no tracking is done after work or outside the controllers' territory.

4.3.6 What is the current state of the technology?

The technology of Bluetooth has been used before to estimate distances for quite a while. A quick search on google results in academic papers from 2011/2012 (example : link).

However, to use this technology for contact tracing is still new. And data protection authorities already acknowledged the risk on false positives due to the circumstances of how radio waves work. For example, people standing close to each other but where there is a thin wall in between, will still result in a close encounter.

4.4 Describe the purpose of the processing

4.4.1 What does the controller want to achieve?

The purpose of the controller will be:

- To create a healthy and safe work environment for its employees
- To have an insight on which parts of the company (location or departments) social distancing is accomplished and to get an idea if there was a problem of too many near encounters
- To be able to give information to the government with regard to contact tracing (or directly or via the employee) when someone is affected
- To monitor if extra safety measures have an effect
- To gather statistical information to learn lessons and take long-term measures to prepare for the next pandemic where social distancing is required
- To make employees aware of the social distancing (the hardware buzzes when an encounter was too close)
- To be able to correct individual employees who do not follow the safety guidelines

4.4.2 What is the intended effect on individuals?

The intended effects are:

- To provide the employees a safe work environment during the COVID-19 crisis.
- To help individuals with their contract tracing after they got infected by the COVID-19 virus.
- To warn employees if they had near encounters in the recent past with someone that was infected by the COVID-19 virus.

4.4.3 What are the benefits for the controller?

The benefits for the controller are:

- Measuring in an objective way how safe the work environment is to proof to the employees that the controller indeed created a safe work environment

- To prevent that multiple co-workers, get the corona virus so that a whole location or department should close.
- To get an insight if extra measures for social distancing need to be taken in some departments/locations

4.4.4 Are there broader benefits?

Yes, an efficient contact tracing will help society to tackle the COVID-19 crisis in an efficient way.

5 STEP 3: CONSULTATION PROCESS

5.1 Which external experts were consulted?

The processor is creating this DPIA so that the controller can use it as input for their DPIA. The processor consulted the following experts:

- Privacy experts from Privatum (www.privatum.be)
- Reseller or Customer experts

5.2 Were the data subjects consulted?

The data subjects were not consulted by the processor. Because it's not in contact with the employees of its end-customers.

We do advise though that end-customers do consult the employees to have an idea if there is willingness or resistance within the company to introduce proximity tracing on the work floor.

5.3 Does the controller need to consult other parties?

In some countries it will be required to discuss and consult the work council or the trade union before implementing the proximity tracing on the work floor because of collective labour agreements or national legislation.

CLEAR DIGITAL however is not responsible to do this consulting, this is up to the controller (the end-customer) to do so.

6 STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

6.1 What is the lawful basis for processing?

It is the controller who should chose the lawful basis. Because of the different guidelines and legislation in each individual country CLEAR DIGITAL can only give some insights per lawful basis.

Lawful basis	Applicable	Reasoning
Vital interest	No	The contact tracing itself is not saving lives. The Belgian privacy authority mentioned in an advice for COVID-19 on the work floor that Vital interest can not be used as lawful basis. (https://www.gegevensbeschermingsautoriteit.be/covid-19-en-de-verwerking-van-persoonsgegevens-op-de-werkvloer)
Legislation	No/Yes?	New Legislation is created very quickly and ad-hoc by governments and differs across countries. For most countries' 'legislation' can't be used as lawful basis even if there are labour laws mentioning it's the responsibility of the employer to create a healthy and safe environment at work. The contact tracing itself is not a necessity to provide this safe environment, it contributes to it. But on its own it's not sufficient. In Germany for example the "SARS-CoV-2-Arbeitsschutzstandard" mentions: "*The employer should have provisions to identify and inform those persons (employees and, where possible, customers) who are at risk of infection through contact with infected persons.* "
Contract	No	The proximity tracing is not required for an employee to do his/her job.
Consent	No/Yes?	Due to the power imbalance between the employee and employer consent can not be freely given. However, in some countries a national privacy law might stipulate that consent is possible when there is a benefit for both the data subject and the controller. For instance, in Germany it is allowed to use consent for an employee to its employer if both share the same interests.
Public interest	No/Yes?	Only when the end-customer is a government it might be possible to user public interest as lawful basis. A private company can not use this, unless it works directly for the government and performs an essential task there.
Legitimate interest	Yes	This is the lawful basis that will be applicable in most cases.

6.2 Does the processing achieve your purpose?

Purpose	Reasoning
To create a healthy and safe work environment for its employees	The hardware devices start to buzz when there is a close encounter. This will make employees aware and will remind them to keep distance during their job. The dashboarding will give insights per location or department to identify "hot spots" withing the company of the controller.
To make employees aware of the social distancing (the hardware buzzes when an encounter was too close)	The hardware devices start to buzz when there is a close encounter. This will make employees aware and will remind them to keep distance during their job.

To have an insight on which parts of the company (location or departments) there could be problems in the work environment where social distancing can be guaranteed	The platform allows to categorise assets in locations or departments. This can give an insight on the hot spots of near contacts within the company of the controller. Because no location is tracked of the near encounter, the platform doesn't know if the encounter itself happened on the location of that department. The more employees work on a department or location, the more effective it will be to spot a possible problem on that location or department.
To monitor if extra safety measures have an effect	The proximity tracings give instant insight that new measures have a positive effect or not. Less traces means that the measure worked. The number of near encounters can be seen on the dashboard in real time.
To be able to correct individual employees who do not follow the safety guidelines	Because each asset (employee) gets a unique ID, the controller can separately outside the platform keep a link between the ID and the employee (= pseudofiction). Through the pseudofiction the controller can retrieve a list of all near encounters within a certain time from and of a certain duration. The IDs with the highest number of near encounters can then be addressed and discuss what could be the cause.
To be able to give information to the government with regards to contact tracing (or directly or via the employee) when someone is affected	Only when the end-customer is a government it might be possible to use public interest as lawful basis. A private company cannot use this, unless it works directly for the government and performs an essential task there.
To gather statistical information to learn lessons and be able to take measures in the long term to prepare for the next pandemic where social distancing is required	The platform offers dashboards using the proximity tracing. Dashboard can indicate that there is a problem of keeping distance between employees at a certain location/department, or at a certain time of day.

6.3 Is there another way to achieve your purpose?

The controller can ask employees to keep distance and install measures to make that possible. But without actually measuring near encounters it cannot conclude in an objective way if the installed measures are working.

Other ways to achieve the purpose of monitoring is:

- Sending out surveys to the employees: but here you don't know if they will answer honestly. There is a risk they might signal problems when there are no problems at all
- Keeping video surveillance on the work floor: but this has an even bigger impact on the privacy of the individuals and not and one can not keep surveillance all the time and continuously and on all sites/departments at the same time

Another way to achieve the purpose of contact tracing is:

- Asking the infected employee with whom he/she had close encounters: it will be extremely difficult in some work situations to remember with whom you had near encounters. In some situations, employees don't even know each other (e.g. on a big construction site where several sub-contractors work with their own employees)

So, the conclusion is, there are other ways, but they won't be so effective as this platform.

6.4 How will you ensure data quality and data minimisation?

Only near encounters are sent from the hardware device to the central server of the platform.

No location is traced, only the fact that two devices were too close to each other.

It is possible to only use a single id for the asset and couple this with the hardware ID. If the controller doesn't keep a separate list that matches the asset id with the employee, the data is processed anonymously. But then only the purpose of monitoring can be used and no contact tracing or correcting individual employees.

6.5 What information will you give individuals?

The controller should inform the individuals. Depending on the implementation the controller may choose to use the platform for a limited number of purposes. For instance, only for the monitoring and not for individual contact tracing.

6.6 How will you help to support their rights?

The employees don't need to install an app, an email address is not needed as well. So, the processor cannot inform the employees. It's the responsibility of the controller to do so.

The platform does provide ways to:

- Do an export of the data per concept: asset, tracings, etc…
- If a total export is needed for one data subject, then a support ticket can be opened to provide a report with all personal data for one data subject.

A data subject can request to delete his/her personal data.

6.7 What measures do you take to ensure processors comply?

The processor performed this DPIA to be fully transparent and to indicate data protection by design and data protection by default is taken into account when developing this platform.

6.8 How do you safeguard any international transfers?

When the platform is installed on premise the data remains at the location of the controller.

When the platform is running as a SaaS the controller can choose a data center in his region.

7 STEP 5: IDENTIFY RISKS AND IDENTIFY MEASURES TO REDUCE THE RISK

The level of a risk contains out if the “likelihood” and the “severity”. A very important element to calculate the likelihood according to the Methodology for Privacy Risk Management of the CNIL is the “ease of identification”. This means how easy is it to identify an individual.

If the controller uses the name or the personnel number of its employees in the PPP-platform then it will be very easy to identify that individual. The “ease of identification” will than be “maximum” if the controller uses the full name, it will be “significant” if they will use a username or e-mail address or social security number. That is why it is **extremely important** that the controller will pseudonymize the data of the employee in the PPP-platform. This means storing only an ID for the asset. And keep a separate list, safely stored with the proper access rights, with a link between the PPP-platform asset ID and the employee.

For the analysis we identified the following levels of risk: HIGH, MEDIUM and LOW

Severity	Serious impact	LOW	HIGH	HIGH
	Some impact	LOW	MEDIUM	HIGH
	Minimal impact	LOW	LOW	LOW
		Remote	Reasonable possibility	More likely than not
		Likelihood		

The explanation of each status is:

- DONE: the control is implemented
- TODO: the responsible still need to decide to implement the control or accept the risk
- TO BE IMPLEMENTED: the responsible decided to integrate this on the platform in a future release, with indication of target release date.
- /: the responsible of the control is out of scope for this DPIA
- WON’T DO: the responsible of the control has decided to not implement the control and accept the risk

7.1 Data subject rights

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Information provided to the data subject (art 13 GDPR)	The data subject should be informed on how the devices work, which data will be gathered or stored, who can see the data and what will happen with the data.	Not providing transparent information to the employee is a violation of the data subject rights	HIGH	When handing over the dedicated hardware devices the data subject should receive information about which data, purposes of usage, lawful basis, categories of recipients, how to execute rights, etc… In some countries because of legislation it might also be necessary for the controller to consult the Works Council or Trade Union The controller can include information of this processing in the internal privacy policy	Controller	LOW	/
Right of access (art 15 GDPR)	The data subject should be able to request access to his/her personal data. And the controller should answer in time	Not providing a copy of the data in time is a violation of the data subject rights	HIGH	Screen shots can be taken from the PPP-platform of detail screens for the employee.	CLEAR DIGITAL	LOW	DONE
		One must be sure of the identify of the data subject before giving the information	Medium	The controller should only give the details of the ppp-platform to the employee itself and check the identity of that employee	Controller	LOW	/

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Right to rectification (art 16 GDPR)	The data subject should be able to request data rectification (e.g. in case of false positive).	If a hardware device is linked to the wrong asset, the wrong employee will be linked to close encounters this could end up on penalizing the wrong person or giving out the wrong close encounters.	High	It must be possible to relink traces with the correct asset after the registration took place	CLEAR DIGITAL	Medium	TODO
Right to erasure of data (art 17 GDPR)	The data subject should have the right to request erasure of the data for instance when an employee leaves the company.	If an employee leaves the company, he or she may request to erase the collected data.	High	The deletion of an asset and its data is possible on the ppp-platform. The delete is a soft delete, meaning the data is still in the database but not shown on the screens anymore.	CLEAR DIGITAL	High	DONE
				The controller should remove the link between the asset on the ppp-platform and the employee in its pseudonymized records keeping and of course not conforming directly identifiable data on the asset in the ppp-platform	Controller	Medium	/
				The deletion of the asset is a hard delete but the data used to have long term aggregate statistics will be kept (# closed encounters / plant or department)	CLEAR DIGITAL	LOW	TODO
Right to object (art 21 GDPR)	The data subject should have the right to object against the processing (for example when processing is based upon legitimate interest)	The platform is not using an app that the data subject can switch off.	HIGH	It is possible to turn the hardware devices off by the employee	Vendor hardware devices	LOW	DONE

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Automated decision making (art 22 GDPR)	If automated decision making is done, the data subject needs to be informed about the possible consequences	Tracing information could be easily used for automatic decision making. However, the ppp-platform is not making decisions itself, the controller can still blindly trust the system and make assumptions solely on the reporting.	MEDIUM	Before taking decisions solely based on the reporting of the tool, the controller will always discuss with the data subject before taking decisions. E.g. Someone that causes a lot of close encounter tracings might work on a spot where it is impossible to avoid them so it's the responsibility of the controller to fix it and the employee should get penalized	Controller	LOW	/

7.2 GDPR Principles

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Specified, explicit and legitimate purpose(s) (art 5.1.b GDPR)	The purpose is formulated specific, explicit defined. It will only be used if an employee has tested positive.	The controller uses this tool when he should not use this. For example, after the pandemic or track behaviour (e.g. how often in the restroom when placing a hardware device on the entrance)	High	Make staff and management aware what the purposes are and that extending those purposes must be discussed with senior management of the controller.	Controller	Low	/
				Turn off monitoring by asking employees to turn in badges when social distancing is not necessary anymore.	Controller	Low	/
				Create a plan on how and when to decommission the platform.	Controller	Low	/

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Lawfulness of processing	The lawfulness of processing might be based on consent in some cases and this requires special conditions (art 7 GDPR)	Due to the power imbalance between the employee and employer consent cannot be freely given. However, in some countries a national privacy law might stipulate that consent is possible when there is a benefit for both the data subject and the controller. Only in those countries, consent will be lawful, in other countries the processing will be invalid. Controller must rely on another legal basis for processing data.	High	Where consent is a lawful basis for processing: provide that the consent is given freely given + document the consent.	Controller	Medium	/
Limited storage duration (art 5.1.e GDPR)	The personal data may not be stored longer than necessary for its purpose.	For the purposes of contact tracing the information on who had a close encounter with who is only useful for a limited period of time. When going back in the past for 3 months ago the data is irrelevant.	Medium	Automatically delete the reference to the assets for traces after a certain period of time (e.g. 1 month, or configurable). So that a user can only see there was a close encounter but not see anymore which encounter. This way the statistics will remain to make long term conclusions.	CLEAR DIGITAL	Low	TODO
Data should be accurate and kept up to date (art 5.1.d GDPR)	Every reasonable step must be taken to ensure that data that are inaccurate are erased or rectified.	The purpose off the device is to detect close encounters. Inaccurate measurements will lead to 'false positives'.	High	Ensure that the hardware device is accurate (up to X meters). The EU requires in it's guidelines for contract tracing an accuracy of 1 meter (see page 15 EU Toolbox - Covid 19)	Supplier of the hardware devices	Medium	/

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
		The circumstances on how the hardware devices is carried along might influence the accuracy. For instance, the Bluetooth signal will be different if someone carries a badge around the neck or puts it in a trousers pocket.	High	Give clear instructions to the employees on how to carry the hardware devices to optimize the accuracy.	Supplier of the hardware devices (to give guidelines and to calibrate) Controller (to give the actual information)	Medium	/
			High	Follow up if the instructions on how to wear the hardware devices are respected by the employees.	Controller	Medium	/
		If an employee loses the hardware device and others find it, they can abuse the found device to create close encounters that point to the employee that lost the device.	High	It's possible to couple an asset to a new device or to remove a current device from the asset	CLEAR DIGITAL	Medium	DONE
				The controller should give instruction on what to do when a device is lots	Controller	Low	/
		If two employees are at the boundary distance of a close encounter and the devices register multiple traces (on, of, on, of) for the same conversation those two employees had. They will get falsely marked having multiple near encounters within a short period of time.	Medium	The raw "close encounter" event does not contain the notion of time. The hardware device sends a signal every 10 seconds. There is functionality built in that multiple "close encounters" with the same asset within one minute as one single "close encounter" trace	CLEAR DIGITAL	Low	DONE

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
		The person handing out a hardware device to an employee could accidently configure the wrong badge with the wrong asset (individual). So, this means that all tracings will be recorded for the wrong individual	High	Functionality in the platform that makes it possible to do a quick test when handing out a badge to an employee. This test will then not be recorded as a "close encounter" but	CLEAR DIGITAL	Low	TODO
		Circumstances might lead to inevitable false positives (e.g. standing behind a plexiglass)	Medium	Functionality in the platform that makes it possible to let an admin user delete a specific close encounter	CLEAR DIGITAL	Low	TODO
		Hardware devices might accidently get switched between employees	High	Foresee a way to personalize the hardware device, so that the employee recognizes its own device	Supplier hardware device Or Controller	Low	/
			High	Before making decisions always do a sanity check if the data was correct. For instance, when providing traced contacts do a check if it's possible that person X encountered person Y at that time.	Controller	Low	/
		The hardware device might run out of battery, so it will stop tracing	High	The hardware device can send battery status and alive messages to the ppp-platform.	CLEAR DIGITAL	Medium	DONE
				The ppp-platform allows for configuring notifications to privileged users	CLEAR DIGITAL	Medium	DONE
				Follow up notifications and reporting and change battery or change device when it doesn't send alive messages anymore	Controller	Medium	/

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
		If many employers use this system. And an external supplier has to deliver something at the location of the controller. If that employer has a device with the same ID as an employer of the controller it will give a false positive. Or when one controller uses devices from different vendors and ids are colliding.	High	Make sure to use significantly large IDs to avoid collisions with IDs. Even across different controllers and different suppliers of hardware devices.	Supplier hardware device	Low	/
Adequate, relevant and limited to what is necessary data (art 5.1.c GDPR)	The data that is gathered should be minimal and proportional.	Constant tracking of employees and knowing their exact location/ their social encounters during the whole day	High	The device will have a button to turn the device on and off.	Supplier of the hardware devices.	Medium	DONE
				The collected data includes contact tracing, but only on the work floor. So, there is no contact tracing in the spare time or private atmosphere of the data subject.	Supplier of the hardware devices Supplier of network infrastructure	Low	/
				Only the close encounters will be stored on the server of the ppp-platform. It is the hardware device that decides what a close encounter is. The controller can configure in the product what the definition is of a close proximity (how far). If everyone respects the social distancing on the work floor no proximities are captured	CLEAR DIGITAL Supplier of the hardware devices Supplier of network infrastructure	Low	DONE

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
		If the ppp-platform is hacked and the tracing information leads directly to the individual this could harm the reputation of that individual if that information is published in public	High	Remove all fields on the asset that directly can lead to an individual. Examples are: ▪ rename the label "name" to "asset id". ▪ Remove the picture field	CLEAR DIGITAL	Low	TODO
		For the intended purposes it's not necessary to register medical data in the platform	High	There is no field foreseen to indicate if an employee got infected or not	CLEAR DIGITAL	Low	DONE
		In some European countries there is an advice from the national data protection authority that an employer may not ask about the medical condition of the employee. And it's only the responsibility of the employee to provide the governmental contact tracers the information of near encounters. Thus, the user should be the only one seeing the proximity contacts.	High	Providing a way for the employee to see its own traced contacts on the portal would require including direct identifiable data within the ppp-platform. This will increase the risk of many other topics. So, the residual risk will be still high.	CLEAR DIGITAL	High	WON'T DO
Integrity and confidentiality (art 5.1.f)	Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing	Limit what users will see in the tool to what they need for their job. Someone that is responsible to monitor safety for one department/plants/sites shouldn't be able to see the data from other departments/plants/sites	Medium	Create a system that supports roles within the ppt-platform so that users can only see data for a specific department, plant or site	CLEAR DIGITAL	Low	TODO
			Medium	Make a difference in roles for read only access and write access	CLEAR DIGITAL	Low	TODO
			High	Make a distinction between roles of users that can see or create aggregated reports and users that can see individual contacts	CLEAR DIGITAL	Medium	TODO

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
		Even if a user need access rights, this doesn't mean that the user can consult that data at anytime. The individual contact traces should only be consulted when that employee asks for it or indicates he/she is infected.	High	Create audit logging to log when a user retrieves or changes details from an individual. This way a separate role (e.g. the DPO of the controller) can check whether the data has not been consulted out of proportion.	CLEAR DIGITAL	Medium	TODO
			High	Implement the 4-eye principle. This would mean in practice that before a user can see contact trace details (who had a proximity with who and when) he/she needs to ask permission to another user (role) to view it. So, the controller could implement then a way that the employee notifies two different roles and if there is a confirmation only then the details can be viewed.	CLEAR DIGITAL	Low	TODO

7.3 Accountability

Here we limit the DPIA only to the responsibility of CLEAR DIGITAL.

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Maintain a procedure for data breaches (art 33 GDPR)	The processor shall notify the controller without undue delay after becoming aware of a personal data breach	The controller must notify the data protection authority within 72 hours	High	Putting an incident management system in place tackling internal incidents as well	CLEAR DIGITAL	Low	?
Keeping records of processing activities (art 30.2 GDPR)	The processor shall maintain a record of all categories of processing activities carried out on behalf of the controller	Not having this register means that the processor has no overview of the processes and activities where it processes personal data.	High	Keeping records of processing activities up-to-date and appointing a responsible to do this	CLEAR DIGITAL	Low	TODO
Impact assessment (art 35 GDPR)	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	Creating a solution without doing an impact analysis may cause the go-live of a product with high risks on the privacy of individuals.	Medium (for the processor)	Executing a DPIA to identify privacy risks within the ppp-platform.	CLEAR DIGITAL	Low	DONE
				Define a process to ensure the technical development lifecycle and product updates trigger the right thresholds for refreshing the DPIA, and what you can do to build this into the sprint cycle. (conform with ICO guidance)	CLEAR DIGITAL	Low	TODO
Data protection by design (art 25 GDPR)	Make sure your design choices enable you to clearly tell your users about any uses of their data that may be unexpected or could	By adding new features on the ppp-platform the privacy by design and by default principles must be guaranteed	Medium	Within any product roadmap or description of objectives and requirements (epics, stories) articulate how the user will	CLEAR DIGITAL	Low	?

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
	have significant effects on them, and if there are any residual privacy risks.			understand, e.g. through the experience and interface design, that their privacy has been engineered into the project. (conform with guidance ICO)			
				Consider how to functionally decouple features. Ensure users are not compelled to share additional data to access existing features or new features, and to allow any features to be rolled back or deprecated. (conform with guidance ICO)	CLEAR DIGITAL	LOW	?

7.4 Organisational measures

Here we limit the DPIA only to the responsibility of CLEAR DIGITAL.

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Confidentiality (art 28 GDPR)	Processors should ensure that persons authorised to process the personal data have committed themselves to confidentiality	Employees or contractors might process sensitive data	High	Putting an incident management system in place tackling internal incidents as well	CLEAR DIGITAL	Low	?
Raising Awareness (CNIL Security guide)	Make each user aware of the privacy and security challenges of the organisation.	The biggest cause on a data breach is a human error. People need to be aware so that they have the knowledge on when to be extra careful	Medium	Raise the awareness of users working with personal data by educating them on the privacy risks, inform them of the measures implemented by their organisation in order to deal with the risks and their potential consequences. Organise awareness raising sessions, regularly send updates on the relevant procedures for the individuals' roles, send them reminders via e-mail, etc.	CLEAR DIGITAL	Low	?

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
				Document the operating procedures, keep them up to date and make them available to all the users concerned. In concrete terms, any action on personal data, whether it is administration-related operations or plain use of an application, must be explained in clear language adapted to each user category, in documents to which the users can refer.	CLEAR DIGITAL	Low	?
				Write an IT charter and enforce its application	CLEAR DIGITAL	Low	?
Ensuring continuity	Make sure that business continuity can be guaranteed	If the controller relies on the platform the processor should guarantee continuity otherwise the safety of individuals may no longer be monitored and guaranteed	MEDIUM	Create an IT business continuity management plan, even if brief, including the list of those involved.	CLEAR DIGITAL	Low	?
Information Management System	Embed information management and data protection within the company	If there are no security procedures the staff will all have their own ways of doing things and this might introduce security risks	MEDIUM	Obtain a documentary base setting out data protection objectives and rules (action plan, regular review of the data protection policy, etc.) and monitor if the rules are followed and review the policies periodically	CLEAR DIGITAL	Low	TODO

7.5 Technical measures

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Authenticating users	To ensure that a user only accesses the data that he/she needs, he/she must be associated with a unique identifier and must authenticate himself/herself before any access to personal data.	Passwords might get hacked or guessed.	High	Create a basic password policy on the ppp-platform that enforces passwords being 8 characters long and having at least letters and numbers.	CLEAR DIGITAL	High	DONE
				Creating a password policy complying to the CNIL standards: 8 long, 3 different character types, and locking the account after 10 invalid attempts	CLEAR DIGITAL	Medium	TODO
				Enable two factor authentication	CLEAR DIGITAL	Low	TODO
				Store passwords securely, at the least hashed with a cryptographic hash function using a salt or a key	CLEAR DIGITAL	Medium	DONE
		System integrators implement the ppp-platform from CLEAR DIGITAL as well, and they need to give the admin password to the controller	HIGH	The admin password for a controller is shown the first time (or on password reset) to the reseller within the application. So, the password is sent over a secure channel (HTTPS with TLS 1.2)	CLEAR DIGITAL	Medium	DONE
				Force users when they are given a password to change the password on first login	CLEAR DIGITAL	Low	TODO

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Securing servers	The security of servers must be a priority as they centralise a large amount of data.	Unauthorized access to the servers	HIGH	Giving the controller the opportunity to do an installation on premise	CLEAR DIGITAL	Low	DONE
		Eavesdropping by a hacker or third party that can intercept the data	HIGH	Implement the TLS 1.2 protocol for encrypted communication in transit for SaaS	CLEAR DIGITAL	Low	DONE
			HIGH	Implementing safe communication channels for on premise installation	Controller	Low	/
Encryption	Make personal data unintelligible to anyone without access authorization	If data is stored in rest on a database and a hacker gains access to that database server data will be visible for an unauthorized person	HIGH	Use encrypted databases for SaaS	CLEAR DIGITAL	Low	DONE
				Use encrypted databases for on premise	Controller	Low	/
Patch management	Make sure all servers and libraries are up to date	When a vendor of a library or server release new versions with security patches these must be installed, or hackers could exploit the vulnerability	HIGH	Install critical updates on the servers	CLEAR DIGITAL	Low	DONE
			HIGH	Track used 3rd party libraries in the software to update automatically (if backwards compatible) and to mark them as fixed if they need to be replaced or refactored in the future development roadmap	CLEAR DIGITAL	Low	DONE
Ensuring continuity	Make sure that business continuity can be guaranteed	If a server or hard disk crashes all the data should be recoverable	MEDIUM	Having a backup schedule in place for SaaS installations.	CLEAR DIGITAL	Low	DONE
				Monitor if back-ups are successful	CLEAR DIGITAL	Low	?
				Periodic test if back-ups are still working for SaaS installations	CLEAR DIGITAL	Low	?

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
				Taking backups, monitoring and periodic test of the backups for an on-premise installation	Controller	Low	/
Audit logging	In order to be able to identify fraudulent access or abusive use of personal data, or to determine the origin of an incident, it is necessary to log certain actions carried out on the IT systems. To do this, logging and incident management measures must be implemented. It must record relevant events and guarantee that these logs cannot be altered. In any cases, these elements must not be kept for an excessive time period.	People abusing their access to perform fraudulent actions.	Medium	Keep minimum audit logging in the database (last update user, last update timestamp)	CLEAR DIGITAL	Low	/
				Set up logs (i.e. storing events in "log files") to record users' activities, abnormalities and events related to security. Accesses should be logged with their identifier, the date and time of their connection as well as the date and time of their disconnection; In certain cases, it may be necessary to also keep information on the actions undertaken by the user, the types of data consulted and/or modified, and the reference of the concerned data.	CLEAR DIGITAL	Low	TODO
		If different people use the same account, it will not possible to know who did what	Medium	Create personal accounts for all users: - support users of the processor - Users of the controller - Support users of the system integrator	CLEAR DIGITAL	Low	TODO

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
End-point protection	To protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of personal data (antivirus, firewall, proxy, anti-spyware, reporting of security events, etc.).	Viruses and crypto lockers could make that data is not usable anymore.	High	Install end-point protection applications on servers and workstations for SaaS	CLEAR DIGITAL	Low	TODO
				Install end-point protection applications on servers and workstations for on premise	Controller	Low	/
Maintenance	Minimize the risk when doing maintenance (fixing bugs, installing new releases)	To limit the likelihood of threats associated with maintenance operations on hardware and software (procurement contract, remote maintenance, user's agreement, erasure of data, etc.).	Medium	Record all maintenance operations in a logbook.	CLEAR DIGITAL	Low	?
			Medium	Govern remote maintenance operations by systematically using encrypted communications channels, use robust authentication keys or passwords, log accesses	CLEAR DIGITAL	Low	?
Anonymization	Remove every link to the individual	When developing new features, developers could take a copy from a production environment exposing all personal data (if present on that environment)	Medium	Make sure all direct identifiable fields are replaced by dummy data on nonproduction environments	CLEAR DIGITAL	Low	TODO
Secure and stable software	Make sure the development process is stable and secure	Unstable releases might cause unavailability of the data	High	Testing a release manual before it goes into production	CLEAR DIGITAL	Medium	DONE
				Perform automated tests, including security testing and the roles/features/etc..	CLEAR DIGITAL	Low	TODO
				Perform periodic pen testing or after big changes that could cause a security risk. The pen test should test the OWASP	CLEAR DIGITAL	Low	TODO

7.6 3rd party risks

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
Build a list of all 3rd party libraries that are used	Having control over the use of 3rd party software	Including malicious code by an obscure 3rd party software library which sends out data. Or introducing unsafe code which makes the whole platform vulnerable.	Medium	Use of coding libraries, frameworks, APIs, SDKs and other software components, including those within the mobile operating system, must be understood and clarified. Collection of data by third parties for other purposes must be avoided. (conform with ICO guidelines)	CLEAR DIGITAL	Low	?
				Limit APIs, database analytics or other data exchange mechanisms to parties that are directly supporting proximity notification delivery. Where access is required for epidemiological reasons for trend/pattern analysis then consider earlier points about purpose limitation and refreshing the DPIA. (conform with ICO guidelines)	CLEAR DIGITAL	Low	?
Build a list of all 3rd parties involved in the	Having control over all parties which process data, ensure that they process the data in a correct manner.	Enabling 3rd parties without the appropriate level of GDPR knowledge and procedures, may lead to several risks such as data breaches, liability claims, etc.	Medium	All 3rd parties involved in the processing must be listed to know which party is responsible for which processing, to know which	Controller	Low	?

Requirement	Description	Description of the risk	Rating of the risk	Controls to mitigate risk	Responsible party for the controls	Residual risk	Status
processing of data				party has access to which data, to know the responsibilities of each party and so on.			
				Data Processing Agreements must be concluded with those 3rd parties.	CLEAR DIGITAL		?
				Data Sub-Processing Agreements must be concluded with system integrators	CLEAR DIGITAL		?