ITEA Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

*ITEA 3 is a EUREKA strategic ICT cluster programme*

# Mental Health and Productivity Boosting in the Workplace

## D2.1 - User and technical requirements, pilot specifications

**Edited by: Diego Fuentes (Hi-Iberia)**

**Date: 30th September 2021**

**Version: V1.0**

**Contributing partners: Diego Fuentes (Hi-Iberia), Omar Nasir (Helvar), Sampsa Puttonen (FIOH), Elena Vildjiounaite (VTT), Davor Stjelja (Granlund), Kimmo Häyrinen (UniqAir), Henrique Figueiredo (Medis), Daesub Yoon (ETRI), Tuisku Sarrala (NIXU)**

# Table of Contents

## Project acronyms

| | |
|---|---|
| GDPR | General Data Protection Regulation |
| HID | Mental Health Information Display |
| MHS | Mental Health Sensing and Processing |
| MWS | Mental Well-Being Support |
| TR | Technical requirement |
| UFR | User functional requirement |
| UIM | User Information Management |
| WEA | Well-Being Effectiveness Analysis |
| | |
| | |
| | |
| | |
| | |
| | |

# 1. Introduction

Mad@Work intends to develop truly unobtrusive, privacy-safe, appealing solutions, smoothly integrated into work environment and appropriate for long-term use in diverse real-life settings. Thereby, it is proposed that Mad@Work solutions are tested in long-term pilots, mainly with knowledge workers and respective HR departments in the partners' workplaces. Additionally, such workers and HR departments must be committed in co-designing the pilots as well as the solutions, so that it is ensured that design and development is carried out in a truly human-centred way, and that the voice of end-users and relevant stakeholders is efficiently heard.

This deliverable *D2.1 - User and technical requirements, pilot specifications,* which is framed within *Task 2.1 - User and technical requirements, security, privacy and ethics,* intends to reflect how the Mad@Work solutions are being co-designed for its use in diverse real-life settings as it is shown in the different pilots. Thereby, it is possible to find along the deliverable many end-user requirements depending on which is the pilot, user stories about how Mad@Work solutions could be applied to different real-life settings (that is, pilots) and even, the ethical and legal way in which workers must collaborate with the co-design, and consequently, with their involvement in the different pilots, among other things. For all this and more, this deliverable starts defining a global methodology to collect as much information as possible about end-users, pilots in partners' workplaces, system components to develop as well as necessary procedures and tools for protecting privacy and respecting ethics.

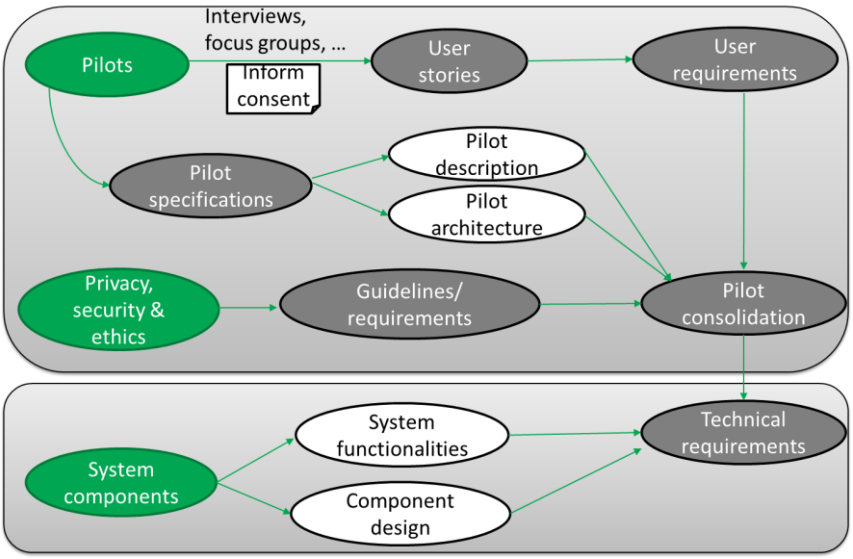



*Figure 1 – Methodology for the deliverable D2.1*

As can be seen throughout the deliverable, the above figure depicts clearly the deliverable structure, so that section 2 is focused on the pilot specifications and the related-user requirements, section 3 is about the system components with the corresponding technical requirements and sections 4, 5, 6 and 7 are about privacy, security and ethics.

Finally, but following with the main objective of this deliverable, it is important to remark that a cross-cultural questionnaire (see Appendix 1) has been prepared by the Mad@Work Consortium in order to help with this co-design, and some preliminary results (see Appendix 2) are already shown.

# 2. Pilot Specifications & User Requirements

## 2.1. Pilot 1 - Stress detection and mitigation in location-independent people working in front of a PC (led by Hi-Iberia)

### 2.1.1. Pilot Description

This pilot intends to deploy and validate part of the Mad@Work platform with people working in front of a PC regardless of their location. Concretely, this pilot aims to:

- Deploy and validate a video-based stress detection system, which will be complemented with online self-questionnaires and physiological data whenever it is possible.
- Assess the mental health, concretely stress and emotions, in people working with their PC through clips of video recorded through their webcam, and in combination with other sources like self-questionnaires or physiological data.
- Validate if an individual support tool can mitigate stressful situations by recommending relaxing activities to the people participating in the pilot.
- Analyse the acceptance and feasibility of the stress detection system and the individual support tool belonging to the Mad@Work platform among the people participating in the pilot.

For a precise mental health assessment based on stress and emotions detection, it will be needed to collect and analyse different kind of data along all pilot phases, that is:

- **Clips of video**, with a duration still to be determined, which will be recorded through the webcam of the monitored people's PC once a recording session is accepted and initiated from the Mad@Work Web App.
- **Online self-questionnaires**, which will be answered through the Mad@Work Web App by each person. Such self-questionnaires will be based on commonly-used questionnaires in laboratory and daily life stress experiments such as:
    - Patient Health Questionnaire-4 (PHQ-4),
    - Perceived Stress Scale (PSS), 10 items (once per month)
    - Stress Self-Rating Scale (SSRS),
    - NASA-TLX,
    - Self-Assessment Manikin and Positive and Negative Affect Schedule (PANAS)
- **Physiological data**, such as ECG, heart rate, respiratory rate, blood pressure, which will be collected from a smart bracelet worn by each monitored people.

This pilot will be carried out regardless the location, either at home or in HI-Iberia office, with 15 knowledge workers approximately, which will be recruited voluntarily from the R&D team and SW Developers team. Such pilot will have four different stages:

- 1st stage: Interviews with knowledge workers from the R&D team and SW Developers teams, as well as interviews with people working in the HR department.

- 2nd stage: Data collection with knowledge workers from the R&D team and SW Developers teams, at least clips of video.
- 3rd stage: Initial testing & evaluation of video-based stress detection system as a unimodal mental health assessment as well as the multimodal mental health assessment in combination with self-questionnaires and physiological data.
- 4th stage: Final evaluation of mental health assessment as well as the individual support tool, which is implemented in the Mad@Work Web App.

### 2.1.2. High-level architecture

As it can be seen in the below figure, this pilot revolves around a Mad@Work Web App with a two-fold purpose:

- Manage the data collection with the monitored people launching the video recording sessions and the online self-questionnaires whenever it corresponds.
- Act as an intervention support tool with the monitored people offering a dashboard to monitor the mental health assessment results and a set of activity recommendations for stress mitigation.

In the back-end side, "intelligence" components will make use of the collected data, which will be stored in the data repository, in order to feed up the individual support tool with the mental health assessment and the activity recommendations.

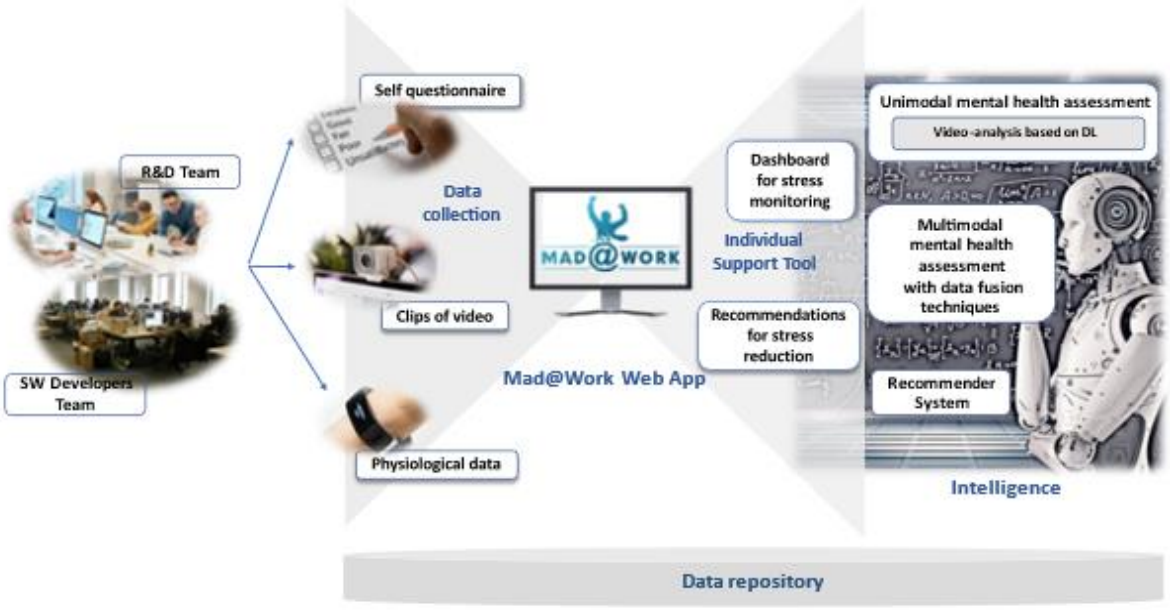



*Figure 2 - Pilot 1: High level architecture*

### 2.1.3. Summary of User Stories

The SW development team uses *scrum* for developing and delivering its SW products, and the corresponding *sprints* take three or four weeks, so there is usually a peak of stress every three or four weeks. Such peaks of stress are sometimes low, but sometimes high, so the Human Resources department is often worried about them. To mitigate these stressful situations, this department has bought the Mad@Work solution, and now it is being offered voluntarily to knowledge workers to monitor their stress levels.

Elena, which has been working at this company for 5 years as a SW developer, has sometimes felt stress episodes, even considering leaving work for a while, so she has started using the Mad@Work solution to monitor their stress and learn how to mitigate it. Then, Elena is currently wearing a smart bracelet during the working hours, which measures her physiological data and sends them to the Mad@Work solution. Additionally, she opens the Mad@Work Web app at least three times per day to record a 10-minutes video session through the webcam to be analysed by the "intelligence" components and so, get a mental health assessment based on video-analysis. Using the same web app, Elena answers an online self-questionnaire about her daily life stress each week, which is stored in the Mad@Work solution. Thereby, based on the physiological data, video sessions and self-questionnaire results, the "intelligence" components can analyse them and provide a multimodal mental health assessment, as well as suggesting to do some personalized activities which help Elena to reduce their stress.

Meanwhile, Elena periodically opens the Mad@Work Web app to check if there are new results related to her mental health and stress levels shown through a friendly dashboard, and if she has any recommendation her some relaxing activity.

After using Mad@Work solution for three months, Elena has learnt to detect when she is feeling some stress episode and how to mitigate it thanks to the relaxing activities recommended by the Mad@Work solution. Elena, who was a person with a poor mental health, has now gained in personal health, work satisfaction and productivity.

### 2.1.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P1-01** | Users should wear a wearable device collecting their physiological data (ECG, heart rate, respiratory rate, blood pressure, temperature) at least during working hours. | Wearable sensors |
| **UFR-P1-02** | Users should record a 10-minutes video-session through the webcam via Web App at least three times per day. | Video data, Web App for data collection |
| **UFR-P1-03** | Users should record a 10-minutes video-session through the webcam via Web App after performing a recommended activity. | Video data, Web App for data collection |

| | | |
|---|---|---|
| **UFR-P1-04** | Users should answer an online self-questionnaire through the Web App once per week. | Self-questionnaire, Web App for data collection |
| **UFR-P1-05** | Users must not access other users' information (physiological data, video sessions and self-questionnaire results) | Data repository, Web App for data collection |
| **UFR-P1-06** | Users should input their user profile and preferences through the Web App. | Web App for data collection |
| **UFR-P1-07** | Users should check their physiological data (raw data) through the dashboard in the Web App | Web App for Individual Support Tool (dashboard) |
| **UFR-P1-08** | Users should check the unimodal mental health assessment based on video-analysis through the dashboard in the Web App | Web App for Individual Support Tool (dashboard), Unimodal mental health assessment |
| **UFR-P1-09** | Users should check the multimodal mental health assessment through the dashboard in the Web App | Web App for Individual Support Tool (dashboard), Multimodal mental health assessment |
| **UFR-P1-10** | Users should check their stress level through the dashboard in the Web App | Web App for Individual Support Tool (dashboard), Unimodal mental health assessment, multimodal mental health assessment |
| **UFR-P1-11** | Users should visualize any kind of data to be shown through the dashboard in the Web App in a periodically way (daily, weekly, monthly) | Web App for Individual Support Tool (dashboard), |
| **UFR-P1-12** | Users should find recommended activities based on their mental health assessment in the Web App | Web App for Individual Support Tool (recommendations), Recommender System |
| **UFR-P1-13** | Users should give feedback about the suitability of the recommended activities suggested (like/dislike) | Web App for Individual Support Tool (recommendations), Recommender System |

| | | |
|---|---|---|
| **UFR-P1-14** | Users should just open the Mad@Work Web app when it is used as individual support tool voluntarily (without any kind of notifications) | Web App for Individual Support Tool |

## 2.2. Pilot 2 – Personalized Lighting in Indoor Work Spaces (led by Helvar)

### 2.2.1. Pilot Description

The goal of the pilot is to evaluate the usefulness of personalized lighting control systems. Overhead lighting will be installed and made available to users via docking stations. Once the user connects their system to the station, they can wirelessly control lighting using a desktop application. The application allows the user to change colour temperature, intensity, apply pre-configured profiles and allow the lighting to follow natural circadian rhythms. The system will anonymously collect usage data, such as lighting settings and desk ID.

### 2.2.2. High-level architecture

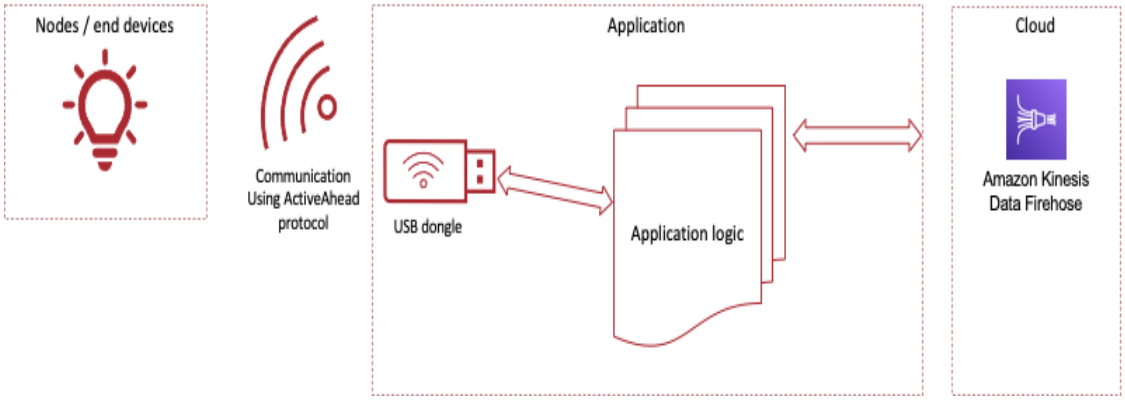



*Figure 3 - Pilot 2: High level architecture*

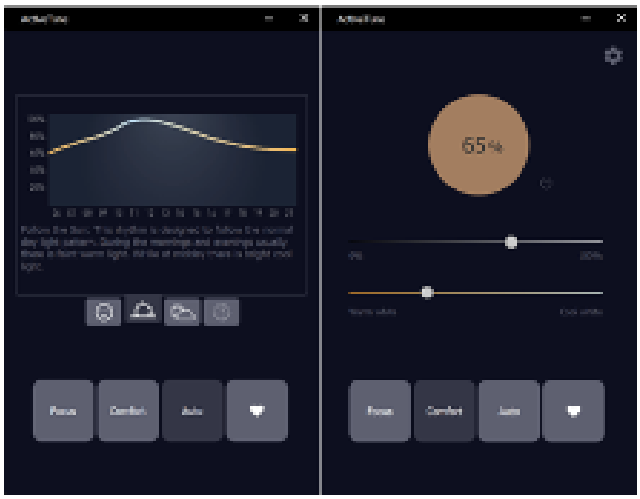



*Figure 4 - Pilot 2: Screenshots of Helvar App*

### 2.2.3. Summary of User Stories

Some conclusions extracted from interviews are as follows:

- Is this the preferred way to control personalized lighting?
- Given that different users have different ways of working, what is the right interface to personalized lighting? Docking station, hand-held device or a laptop without docking station?
- For users who prefer greater control over personalized lighting, has the system improved their productivity/mood and has it brought an overall net positive impact on their day-to-day work?

### 2.2.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P2-01**<br>**Helvar ActiveAhead** | The luminaires installed must be Helvar ActiveAhead. | Helvar AA |
| **UFR-P2-02**<br>**BLE USB Dongles** | The work desks with docking stations must have connected USB dongles which have been configured to communicate with their end-device. | Helvar Support |
| **UFR-P2-03**<br>**ActiveTune Computer** | The application itself is to be installed on user computers. | Helvar App |
| **UFR-P2-04**<br>**Data analysis** | Data analysis on collected data from applications | Helvar Support |

## 2.3. Pilot 3 – Stress and performance in location independent office workers (led by FIOH & VTT)

### 2.3.1. Pilot Description

This pilot intends to develop methods to evaluate mental conditions of people working on PC in offices and during remote work. Aims of the study:

- To develop methods to assess mental conditions of knowledge workers utilizing data from computer, mobile phone and/ or environmental sensors, **with the main focus on detecting long-lasting troubles**. Specifically, we will
    1. collect long-term real-life data from the above-mentioned sensors, as such databases do not exist;
    2. collect self-reports on stress, work content, productivity and (optionally) stressors;
    3. collect physiological data;

4. study correlations between various self-reported factors in long term, e.g., between stress and productivity, or between stress and social factors, as well as correlations with physiological parameters;
5. develop methods to detect long-lasting stress and/or other aspects of mental conditions from the self-reporting questionnaire (e.g., satisfaction with work content, own productivity or self-reported stressors);
6. assess accuracy of the developed methods at different time granularity;
7. evaluate concept and designs of continuously running organisational barometer;

- To develop and to evaluate gamification methods for motivating knowledge workers to participate in data collections and organisational barometer, because drop-out of data collections is a common problem for employee engagement surveys, as well as in other domains, e.g., health promotion and crowdsourcing.

Initially, we planned to collect data from environmental sensors in the offices, but due to COVID, we adapted the pilot plan to include sensors, suitable for remote work. We plan to conduct an initial pilot for remote work conditions and then, pandemic situation permitting, a pilot in offices.

Initial pilot will include 50-60 volunteers, knowledge workers (e.g. professionals, scientists, educators, and information system designers) from VTT and Finnish companies and work organisations. In addition to continuous self-reporting, the participants will be asked to answer pre-study and post-study questionnaires regarding: a) background information), b) health and health behaviour c) work resources demands, recovery and stress, cognitive failures d) post- study survey on participation motivating factors, including the role of gamification.

During the field phase of the initial pilot, the following data will be collected:

1. Objective physiological stress parameters measured are heart rate variability (HRV) and salivary stress markers.
2. Self-reporting on workdays, the following questions: stress level, work content and skills needed, appraised productivity of the day, and work-related reasons for stress/emotions. Also place of work, working times and sleep are queried and cognitive information processing in tested.
3. Smartphone usage data will be collected using an application installed in Android smartphones. The smartphone usage data is pseudonymized by categorizing application names into seven application categories.
4. Computer usage data will be collected by a custom application installed in the participants' computers. Data is pseudonymized by categorizing application names into seven application categories. Contents of the keyboard strokes is not collected, only timestamps of pressing/ releasing the keys.

Choice of sensors in the next pilot will depend on pandemic situation and on how knowledge workers will return to the offices, but the goal is to collect more multimodal data, to develop multimodal fusion methods and to evaluate next design iterations of the org. barometer.

### 2.3.2. High-level architecture

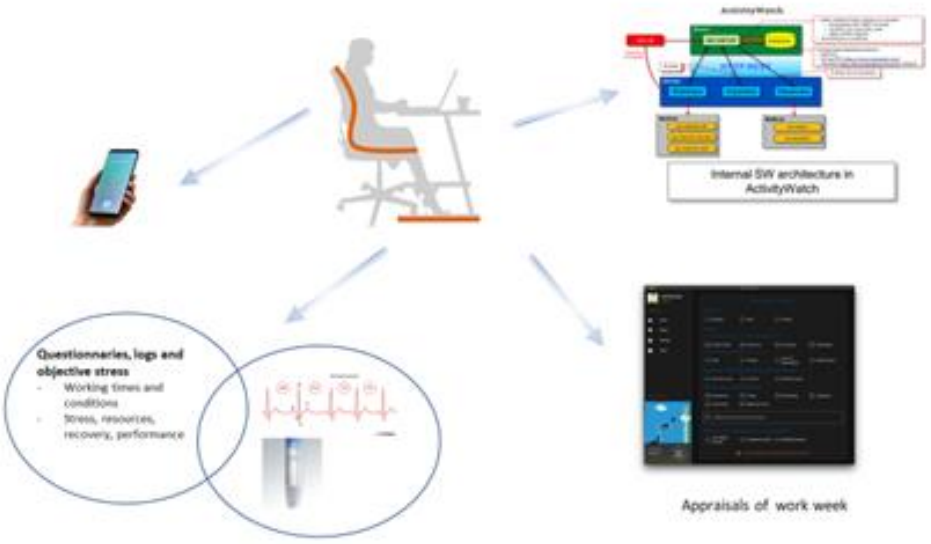



*Figure 5 - Pilot 3: High-level architecture*

As it can be seen in the above figure, this pilot has three-fold purpose:

- To manage the data collection from sensors and from self-reporting questionnaires.
- To provide gamified interaction as additional motivation for the study participants and to study its feasibility for including into organisational barometers and for commercialisation in other domains
- To enable design of org. barometer as an indicator of organisational work culture

In the back-end side, server and various data collection and communication components will enable data acquisition, acquisition of self-reports, gamification and secure storage of the collected data. Later, developed AI methods will enable data analysis, and developed visualisation methods will enable displaying the results in the org. barometer.

### 2.3.3. Summary of User Stories

Org. barometer shows anonymous aggregated stress level of the team and also anonymous aggregated stress levels of persons on two sides of stress median, i.e., stress levels of “the most stressed part” and of “the least stressed part”, without revealing identities of the persons in each group.

Team leader checks org. barometer on a monthly basis. Last check demonstrated that although average stress level of the team did not change, stress of the most stressed part increased. Thanks to the data from previous years, org. barometer suggests that it might be due to the approaching deadline of one financial instrument, important for this team. Thus during the next coffee break the team leader asks whether anybody could help with this type of work. Couple of team members volunteer, and three senior team members, who are dealing with that particular financial instrument, share their workload with the volunteers.

The team leader does not know whether the org. barometer was affected by the stress of all of these senior team members or just one of them, but he is anyway happy that the volunteers learn new skills. Next time, when the team leader checks the org. barometer, stress levels of "the most stressed part" and of "the least stressed part" return to close-to-normal situation, and the team leader knows that he made the right decision just in time to avoid overloading of senior team members.

### 2.3.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P3-01**<br>**Mental stress assessment** | questionnaires and logs | E-questionnaire app and Movisens-xs app |
| **UFR-P3-02**<br>**Computer logs** | User needs to install an application that logs mouse and keyboard usage and sends data to VTT server. User should authenticate herself and allow data transfer. | VTT app |
| **UFR-P3-03**<br>**Phone usage (optional)** | User needs to install an application that logs application usage and reminds to fill a questionnaire. User needs to authenticate herself and allow app access to the data and data transfer. | VTT app |
| **UFR-P3-04**<br>**work stress appraisals (Individual tool) Organisation barometer (HR tool)** | User needs to install an application that prompts to submit self-reports. Users need to answer the self-reports on workdays, 3-5 times a week. The self-reports contain daily and weekly stress and causes of stress and motivation. | VTT app |
| **UFR-P3-05**<br>**Physiological stress assessment** | Heart rate and stress biomarkers | FirstBeat Bodyguardsensor and salivary marker analyses at FIOH |
| **UFR-P3-06**<br>**Mental performance assessment** | Cognitive performance | FIOH test App |

| | | |
|---|---|---|
| **UFR-P3-07**<br>**Environmental sensors** | After return to the offices, users should allow to install IEQ sensors (e.g., temperature, humidity, noise, motion) in their offices | VTT app |
| **UFR-P3-08**<br>**Privacy** | Users should not have access other users' information (computer and phone data, self-questionnaire results and environmental sensors, if applicable) | Data repository and apps for data collection |
| **UFR-P3-09**<br>**Privacy** | Users should have access to own data and should be able to see/ modify/ delete it, as well as to stop data collection any time | Data repository and apps for data collection |
| **UFR-P3-10**<br>**Battery/ data savings** | Users should be able to stop data transfers any time, e.g., to save battery or if on metered network. | Data repository and apps for data collection |
| **UFR-P3-11**<br>**Evaluation** | Users should respond to post-study survey and provide feedback on data collection, gamification and org. barometer concept, along with responses to the questions regarding user personality, such as demographic data, work position etc. | Online questionnaire |

## 2.4. Pilot 4 - Learning facility (led by Granlund)

### 2.4.1. Pilot Description

The goal of this pilot is to develop a scalable solution which finds and recognizes the problems in building's operation in real time. The pilot building is a hospital building in Vaasa and the focus are the spaces which are used by hospital staff. Special focus in on the problems which might affect occupant wellbeing such as bad indoor air quality. For a successful building operation, occupancy information is needed, which is on the other hand very rarely available. Analysing the energy and indoor air quality can answer us the occupancy patterns on the room, zone or a building level. At the same time, while monitoring the occupancy in the room, we can try to answer the questions about the ventilation performance and the effect on the indoor air quality. Which can also be used for tracking the exposure of occupants to the indoor air pollutants.

To make machine learning based analytics scalable we will use semantic web principles. Additionally, in the pilot we will work with students to develop a sensor with the purpose of detecting people, recognizing their activities and possibly stress level. Also, a staff mental stress assessment will be piloted together with VTT in the pilot hospital.

### 2.4.2. High-level architecture

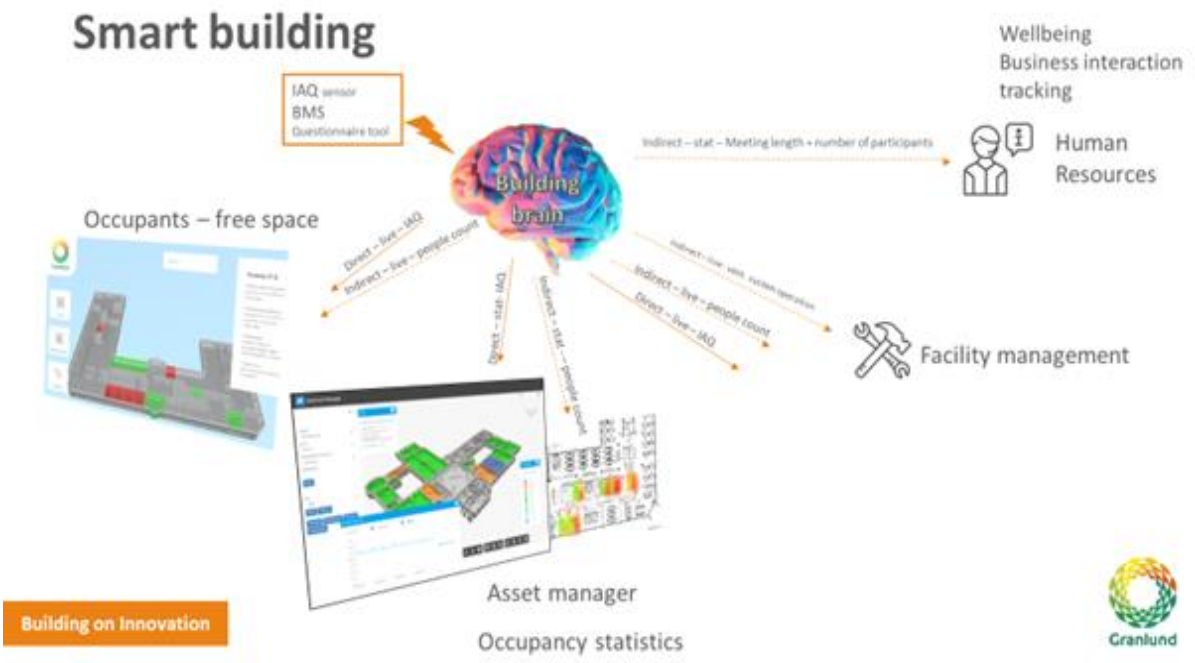



*Figure 6 - Pilot 4: High-level architecture*

### 2.4.3. Summary of User Stories

Idea is to provide a building which will provide good quality of indoor environment, without the need of users to report problems after they happen. Negative changes in the operation of HVAC system will be noticed on time and reported to right stakeholders. Utilisation of the spaces will be reported for the purpose of making them more optimised for user needs. Furthermore, exposure of occupants and interactivity level (e.g., number of meetings, their duration and occupancy) withing organisation will be reported to the human resources.

### 2.4.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P4-01**<br>**Wellbeing & IAQ assessment** | questionnaires and logs | VTT app |
| **UFR-P4-02**<br>**Room AI** | AI which analyses the correlation between IAQ, HVAC system and occupancy | IoT sensor, BMS connection, AI algorithm |

## 2.5. Pilot 5 – Safe to breath (led by UniqAir)

### 2.5.1. Pilot Description

Pilot monitors workers placing via Empathic Building platform and study if and how the presence of air purifiers affects on which office desk people choose. Pilot also monitors the experienced wellbeing by questionnaire tool. Gathered data will be analysed for any correlation between Air Quality, wellbeing experience and presence of purifiers.

### 2.5.2. High-level architecture


*Figure 7 - Pilot 5: High-level architecture*

### 2.5.3. Summary of User Stories

Piloting the effect on experienced/monitored wellbeing when air purification is deployed in knowledge work office environment.

- Can improved air quality be noticeable as lower stress levels?
- What correlations can be discovered?
- Effect of positioning of purifiers
- Effect of level of impurities

Users benefit both physically and mentally when verified air purification is implemented in their working environment.

- Physical benefit comes in a form of verified decrease of air contaminants
- Mental benefit comes from a knowledge of deployment of verified air purification system. Workers are able to rely on safeness of breathing air.

- Users get automated system to ensure safe indoor air or they are getting recommendations to increase or decrease the purification level according to sensor (presence, occupancy level, IAQ/OAQ) data.

### 2.5.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P5-01**<br>**User presence in pilot environment** | Users should be present in pilot office environment. 10-20 users. | Open office environment |
| **UFR-P5-02**<br>**Freedom to choose work desk** | Users should have a possibility to pick the work desk/seat freely. If not, then purifiers´ locations are changed during pilot period. | Office environment without fixed work desks |
| **UFR-P5-03**<br>**Questionnaire app for Users** | Users should fill in a wellbeing questionnaire on how they feel (stress level, overall wellbeing, energy level, etc.) | VTT self-reporting app |
| **UFR-P5-04**<br>**UniqAir purifiers with IoT monitoring** | UniqAir air purifiers to provide pure and safe air for workers | UniqAir purifiers, IoT-platform |
| **UFR-P5-05**<br>**OAQ/IAQ sensors** | Measured air quality data from sensors | FMI OAQ data, SmartWatcher IAQ sensors |
| **UFR-P5-06**<br>**Haltian's Empathic Building test office** | Pilot environment with Empathic Building platform to monitor the presence of workers | Haltian Empathic Building office |
| **UFR-P5-07**<br>**Correlation analysis** | Analysis of possible correlations of purifiers, air quality measurements, workers presence and experienced wellbeing | VTT support |
| **UFR-P5-08**<br>**Depth cameras** | Monitoring of stress levels with depth cameras | VTT depth camera system |

## 2.6. Pilot 6 - Early Detection of Stress in the Workplace (led by Médis)

**Important Note**: *The whole pilot plan and details are dependent on the privacy and data protection analysis that is being performed by Ageas/Médis' DPO, Compliance and Legal teams, in collaboration with other partners. Pilot details might change after this analysis is finalized.*

### 2.6.1. Pilot Description

In this pilot, the deployed solution will be composed of five main components:

1. Video-based tool, which tracks certain variables through the user's face recognition (perceived emotions, pupil diameter, eye gazing, eye blinking, heart rate variability and facial expressions).

2. Self-assessment questionnaires, which will be answered by the user at the end of the period during which he/she was monitored by the video-based tool. The objective is to obtain feedback from the user about how he/she felt during the work period. The questions complement and confirm the data collected by the video-based tool.
3. Self-assessment scales, which will be answered by the user to assess mental health disorders (e.g. stress, anxiety, depression) and workload on a monthly basis. The main goal of these scales is to monitor the subject throughout the pilots' period with longer standard/validated scales.
4. Organizational barometer, to inform managers and team leaders of stress levels in their teams (important note: this information is always anonymized and aggregated)
5. In situations in which high stress level is detected, there will be a recommendation system – a mental wellbeing and health support system with mental health professionals to help the user cope with stress (the details of the recommendation system are still to be finalized)

During the pilot, the videos will not be collected or analysed. The data collected is:

- The reading of the variables analysed through face recognition, as stated in the first paragraph
- The calculated stress level for each user/employee periodically
- Users' answers to the self-use questionnaires

The main objectives of this pilot are to:

- Understand if the video-based tool developed has the capability of correctly assessing employees' stress level
- Validate which information should be shared with the employee regarding his/her own stress level, and at what frequency
- Validate which information (aggregated and anonymized) should be shared with employees' managers, and at what frequency
- Identify users' privacy concerns and possible improvements/changes to the solution to deal with them
- Validate the proposed mental wellbeing and health support system and identify improvements
- Collect employees' and managers' feedback and inputs regarding the solution deployed, to understand if they would use it and in which circumstances

The pilot will be done with 20-40 Ageas' employees (knowledge workers in the insurance industry) from different business units. The employees have not been selected yet, but they will be voluntarily participating in the pilot. The pilot will be performed through the employees' laptop, either in the office or at home.

### 2.6.2. High-level architecture

The architecture is logically divided into three main components that encapsulate a set of features and tasks:

- The first component, data acquisition, is on the user-area and provides several features about the employees' behaviour. It contains a video-based application that collects, in a non-intrusive way, physiological features of the workers such as, perceived emotions, pupil diameter, eye gazing, eye blinking, heart rate variability and facial expressions. Besides this application, the employees will answer a questionnaire twice a day, the main goal of which is to collect their perception of how stressful the work period was and complement the data collected through video.
- The second component of the architecture is on the server side of the system. It is responsible for the consolidation of the data and its persistence in a database. Moreover, it allows for behavioural models to be trained based on the data and using machine learning algorithms to predict mental health conditions, concretely stress of knowledge workers.
- Finally, the third component of the architecture includes a recommendation system that, using the behavioural models and data collected by the video-based application, predicts in real time if the worker will be in stress, informs the worker about his personal state and provides him with personalised stress mediation recommendations such as mindfulness, meditation, coaching, taking a break, among others.

### 2.6.3. Summary of User Stories

Miguel (Médis employee) starts working at 9 a.m. on a Monday. He turns on his laptop and is informed that the Mad@Work video-based tool is ready to be activated. Miguel has to give a clear consent that the Mad@Work tool can be activated and start collecting data. After the consent is given, the tool starts collecting information about Miguel's perceived emotions, eye gazing, heart rate and eye blinking throughout the day, through the laptop's webcam. Miguel is always free to turn off the tool at his own will, whenever he wants.

Miguel is daily (periodicity to be confirmed) informed of his stress status (simple information, like a traffic light) and gets recommendations from the system as to how he can control and reduce his stress levels. Throughout the day, Miguel will also get pop-up notifications requesting him to answer some quick questions. These questions are related with the perceived stress he's feeling through the day, and the reasons for this stress.

Monthly, Miguel will be asked to fill a questionnaire that includes self-assessment scales. These scales will assess his mental health state, such as his level of stress, anxiety, depression, as well as his workload level.

Moreover, weekly (periodicity to be confirmed) Miguel's manager will receive aggregated anonymized data regarding stress levels of the whole team, so that he/she can understand how the team is feeling overall.

If the Mad@Work tool detects high levels during a long period of time, Miguel will be recommended to talk with a mental health professional (psychologist), to help him cope with it and avoid more complicated situations in the future

### 2.6.4. User Requirements

| Requirement ID | Description | Dependencies |
|---|---|---|

| | | |
|---|---|---|
| **UFR-P6-01** | Mad@Work video-based tool has to be installed in users' laptops. | IT Ageas, video-based tool |
| **UFR-P6-02** | Mad@Work video-based tool will need to be connected with laptop's webcam and have the capability to collect information regarding perceived emotions, eye gazing, heart rate and eye blinking | Video-based tool |
| **UFR-P6-03** | The user has to give clear consent before the video-based tool starts analysing the required variables. Without user's consent, the tool cannot perform any analysis or collect any data | User consent |
| **UFR-P6-04** | The user is free to turn off the Mad@Work video-based tool at any time. When the user choses to turn it off, the tool must immediately stop collecting data, until it's turned on again | Video-based tool |
| **UFR-P6-05** | Throughout the day, the user will receive pop-up notifications to answer simple questions about his perceived stress and the reasons for it | Self-assessment questionnaires |
| **UFR-P6-06** | Daily (periodicity tbc), the user will get a simple report about his stress situation (in a clear way, like a traffic light), as well as high-level recommendations on how to control or decrease stress | User individual tool |
| **UFR-P6-07** | Users' managers will receive aggregated anonymized data regarding stress levels of their whole team | Organizational barometer |
| **UFR-P6-08** | If a situation is detected where a user shows high levels of stress, he/she will get relevant recommendations, including talking with a mental health professional (psychologist) | Mental wellbeing and health support system (recommendation system) |
| **UFR-P6-09** | The user is the only one that can have access to the specific results about his/her stress level. No one else shall have access to this information | - |
| **UFR-P6-10** | The Mad@Work tool should not store any video recordings. The only data stored are the readings of the variables analysed (perceived emotions, eye gazing, heart rate and eye blinking), the calculated stress level, and the answers to the self-used questionnaires | Video-based tool |

## 2.7. Pilot 7 - Pilot *WellMind* (led by ETRI)

### 2.7.1. Pilot Description

To manage the mental health conditions of knowledge workers, various environments should be established where their mental health can be continuously monitored and tracked, and take steps to recover from stress. The pilot system measures mental health by collecting biometric information, working environment information, schedule information, and questionnaire information of knowledge workers during their working hours. If the level of stress persists high, the pilot system guides knowledge workers to be treated by mental well-being/health solutions.

Physiological data can be collected through wearable devices such as Samsung Watch. We collect and use Heart Rate and IBI (Inter-Beat Interval) data. We periodically collect and use environmental information such as temperature/humidity, noise, and CO2 concentration.

The questionnaire information is collected by web-based surveys or app surveys according to the situation of knowledge workers. The questionnaire can be composed of a profile questionnaire that you only need to answer once, job stresses that you respond periodically, and general stress questionnaire.

We evaluate the stress index of knowledge workers using biometric information, periodic questionnaire information, environmental information, and schedule information.

A pilot test is conducted in a laboratory where ETRI's knowledge workers work. We plan three scenarios for the pilot test as follows:

- Scenario for collection and analysis of the mental health data in the workplace.
- Scenario for mental well-being/health support in the work environment
- Scenario for statistical analysis and retrieval of mental data for workers

ETRI's knowledge workers who conduct research related to information, communication and convergence technologies will participate in the pilot test.

### 2.7.2. High-level architecture

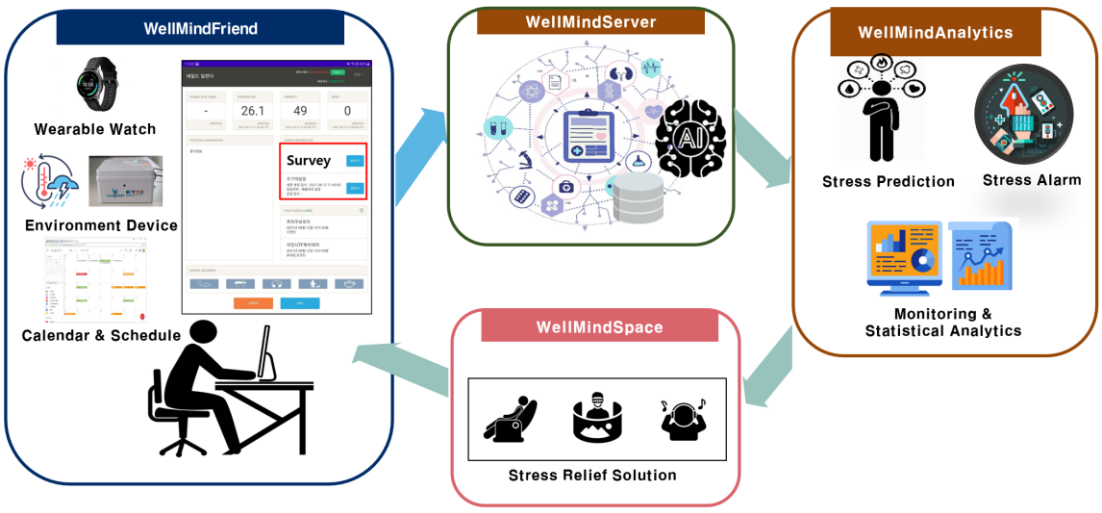



*Figure 8 - Pilot 7: High-level architecture*

The WellMind system consists of 4 conceptual components: WellMindFriend, WellMindServer, WellMindAnalytics, and WellMindSpace. WellMindFriend collects self-identified data and lifelog data, and screen contents. WellMindServer deals with data processing and data storage. WellMindAnalytics are focusing on AI-based data analytics and monitoring. Finally, WellMindSpace provides stress relief solutions such as a massage chair, VR, and etc.

### 2.7.3. Summary of User Stories

Upon arrival at work, Mr. Kim unlocks the tablet and activates the Mad@Work “Wellmindfriend” application (hereinafter referred to as WFriend). After checking the tasks scheduled on that day and stress estimation, he starts working. The cheering message can be displayed on the screen all the time with the current stress index. When a regular push notification appears, he responds to physiological data measurement and surveys. His subjective and physical stresses can be measured through surveys and analyses of his bio-signals. In addition, various data obtained from environment sensors and work schedules could be collected. Based on such data, AI-based analysis can provide a comprehensive understanding of the stress status and the monitoring results that come with tailored mental well-being/health solutions. He sometimes clicks the “Stress” button he feels stress. The “WFriend” app offers a suitable solution considering the work schedule and available solution depending on the choice of the user. He accepts and follows the provided stress relief solution such as a massage chair, a nap, music, eye massage, a walk, stretching, funny videos, etc. With the help of the “WFriend” app, Mr. Kim with poor mental health can be given a stress relief solution together with visualized data. He can also take a break when needed for improvement of work satisfaction, productivity, and personal health.

### 2.7.4. User Requirements

This section describes user requirements for AI-Based Mental Health & Mental Well-Being Management Solution for Knowledge Workers and aims to determine the scope and content of the final results of the task.

The WellMind system can be categorized into 6 major functionalities:

- User information management manages user and organization registration, and data access authorization.
- Mental health sensing and processing collects and stores information of a survey, a working environment, schedules, bio-signals, etc.
- AI-based methods for mental health analysis and assessment.
- Mental health information visualization displays the working environment information, physiological data, and detailed stress data.
- Mental well-being/health support setups the type of stress relief solutions based on user preferences. The mental health support also offers a tailored solution by identifying the condition that requires the solution.
- Mental well-being/health effectiveness analysis measures and displays the stress-relief effectiveness after using (experiencing) the solution.

We have two kinds of actor: a user and a task manager. A user is a knowledge worker who uses the mental health/well-being service. The user registers as a membership for the service and provides the system with the required information for stress measurement including profile, physiological data, and a survey. The system will measure the user's stress status and provide an appropriate stress relief solution. A task manager manages the organization consisting of users who have a membership for the service. The task manager receives users' stress data from the mental/well-being system to monitor and manage their stress.

*User Information Management (UIM)*

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P7-UIM-001** | Users should be able to input information for their individual profiles. | UIM |
| **UFR-P7-UIM-002** | Users should be able to apply for memberships. | UIM |
| **UFR-P7-UIM-003** | Users and Task Managers should be able to edit the membership information. | UIM |
| **UFR-P7-UIM-004** | Users and Task Managers should be able to terminate their memberships. | UIM |
| **UFR-P7-UIM-005** | Users should not be allowed to access the other users' information (data). | UIM |

*Mental Health Sensing and Processing (MHS)*

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P7-MHS-001** | Users should be able to take a survey on a regular basis during their work hours. | MHS |
| **UFR-P7-MHS-002** | Users should be able to take a daily survey during their work hours before leaving the office. | MHS |
| **UFR-P7-MHS-003** | Users should be able to measure their bio-signals (e.g., heart rate and temperature). | MHS |

*Mental Health Information Display (HID)*

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P7-HID-001** | Users should be able to check their bio-signal data (e.g., heart rate and temperature). | HID |
| **UFR-P7-HID-002** | Users should be able to check their working environment data (e.g., temperature, humidity, noise, $CO_2$, movement, etc.). | HID |
| **UFR-P7-HID-003** | Users should be able to check the integrated stress index. | HID |
| **UFR-P7-HID-004** | Users should be able to check detailed stress data (e.g., survey questionnaires, schedule, working environment index, physiological index, etc.). | HID |
| **UFR-P7-HID-005** | Users should be able to receive a notification when stress is detected. | HID |

| | | |
|---|---|---|
| **UFR-P7-HID-006** | Users should be able to check the information about their stress when it is detected. | HID |
| **UFR-P7-HID-007** | Users should be able to check the status of stress related to the information that they input most recently in the self-report.<br>(e.g., the status of stress and energy). | HID |
| **UFR-P7-HID-008** | Users should be able to search their stress status information periodically (e.g., a day, a week, a month).<br>* Examples of the stress status information: subjective stress index, physiological stress index, energy index, the number of clicks on the stress button, etc. | HID |
| **UFR-P7-HID-009** | Users should be able to check the visualized analysis of stress. | HID |
| **UFR-P7-HID-010** | Task managers should be able to check the history of other members' stress data. | HID |
| **UFR-P7-HID-011** | Task managers should be able to check the stress-relieving guide for members. | HID |
| **UFR-P7-HID-012** | Task managers should be able to receive a notification when the stress of members surpasses the threshold. | HID |
| **UFR-P7-HID-013** | Users should be able to check the daily schedule (of meeting, training, work, etc.) and estimated data about the stress of the day on their WellMind display. | HID |

*Mental Well-Being Support (MWS)*

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P7-MWS-001** | Users should be able to edit their preferable encouraging phrases. | MWS |
| **UFR-P7-MWS-002** | Users should be able to check (or read) the encouraging phrases at all times. | MWS |
| **UFR-P7-MWS-003** | Users should be able to set up their preferred type of stress relief solutions. | MWS |
| **UFR-P7-MWS-004** | Users should be able to receive a stress relief solution automatically<br>(e.g., for long hours of sitting, consistent stress, or continuous alerts for environment data). | MWS |
| **UFR-P7-MWS-005** | Users should be able to respond to whether they have used the stress-relief solution. | MWS |

*Well-Being Effectiveness Analysis (WEA)*

| Requirement ID | Description | Dependencies |
|---|---|---|
| **UFR-P7-WEA-001** | Users should be able to measure the effectiveness of the stress relief solution after they used or experienced it (e.g., by measuring bio-signal for five minutes or taking a survey about the level of satisfaction). | WEA |
| **UFR-P7-WEA-002** | Users should be able to check the stress relief effectiveness. | WEA |
| **UFR-P7-WEA-003** | Users may not accept and refuse a stress relief solution. | WEA |
| **UFR-P7-WEA-004** | If users do not accept using the stress relief solution, they should be able to skip the measurement of the effectiveness of solutions. | WEA |
| **UFR-P7-WEA-005** | Users should be able to check the information of the stress relief solution that they previously used. | WEA |

# 3. System Components & Technical requirements

## 3.1. Pilot 1 - Stress detection and mitigation in location-independent people working in front of a PC (led by Hi-Iberia)

### 3.1.1. Sensors

***Smart bracelet (wearable device)***

*Description & System functionalities*

A low-cost commercial wearable device (*Smart Bracelet Watch E66*) is used to collect physiological data from each of the monitored people participating in the pilot. Concretely, relevant physiological data are ECG, heart rate, respiratory rate and blood pressure.

Particularly, this wearable device requires to send monitored people's physiological data via Bluetooth to the monitored people's mobile phone for further processing by a mobile application developed by HI-Iberia outside the project scope. So, data are stored in HI-Iberia's servers in order to avoid problems with the protection of user data.

| Functionality ID | Description |
|---|---|
| **FUNC-01** | Collect monitored people's physiological data such as ECG, heart rate, respiratory rate, blood pressure |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-01** | The wearable device must collect data during video recording sessions. |
| **TR-P1-02** | The wearable device shall collect at least heart rate and ECG data. |
| **TR-P1-03** | The wearable device requires user to install on his/her mobile phone an application for the correct processing and storage of the data on HI-Iberia's servers. |

### 3.1.2. Data collection

***Video data collection***

*Description & System functionalities*

Video data collection is performed through a Mad@Work Web App which allows monitored people to record and store videos through the own webcam. Such recording sessions are launched voluntarily, and the corresponding clips of video have a maximum duration of 1 minute, feature which is managed by the Mad@Work web app by stopping the video recording session when it is reached. Additionally, when the recording session is finalized, and before storing it, Mad@Work Web App requires the monitored people to express whether you felt "relaxed" or "stressed" in order to tag the video and facilitate further training of the algorithm. All clips of video are stored in the data repository with its corresponding date and tag following the privacy, security and ethical specifications.

| Functionality ID | Description |
|---|---|
| **FUNC-02** | Collect and store monitored people's video recording sessions through the own webcam in the PC. |
| **FUNC-03** | Tag all video recording sessions in order to build a complete dataset which serves to train algorithms for data analysis. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-04** | The duration of each video session will not exceed one minute |
| **TR-P1-05** | Each video recording session must have:<br>- A well-lit working place, where the person can be correctly identified.<br>- A recording plane centred on the face of the person being recorded.<br>- No appearance of other persons in the same video session. |
| **TR-P1-06** | For each video clip the following information shall be stored:<br>- Identifier<br>- Date the video was recorded<br>- Tag annotation |
| **TR-P1-07** | The video clip shall be recorded at a minimum frame rate of 20 fps. |
| **TR-P1-08** | The video clip shall be tagged when finalizing the recording session. |

***Self-questionnaires***

*Description & System functionalities*

Self-questionnaires are performed through a Mad@Work Web App once per week. These self-questionnaires are based on questionnaires commonly used in stress experiments like Perceived Stress Scale (PSS) and they aim to collect extra information (stress, emotions, health status) from the monitored people along each week.

| Functionality ID | Description |
|---|---|
| **FUNC-04** | Collect and store extra information from the monitored people which serves to assess long-term mental health |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-09** | Self-questionnaires shall be launched once per week by the Mad@Work Web App. |
| **TR-P1-10** | Self-questionnaires shall follow the Perceived Stress Scale (PSS) questionnaires |

### 3.1.3. Data processing & Intelligence

***Unimodal mental health assessment based on video analysis***

*Description & System functionalities*

A video-based stress detection system is being developed to assess the mental health, concretely stress and emotions, in people working with their PC from clips of video. Such system intends to combine clips of video and physiological data in order to detect stress episodes making use of deep algorithms for video data analysis. Additionally, this video-based stress detection system will provide a private self-diagnostics of stress episodes which helps monitored people to keep a good mental health.

| Functionality ID | Description |
|---|---|
| **FUNC-05** | Assess stress (yes/no) in real time in people working with their PC through short video sessions recorded through their webcam |
| **FUNC-06** | Assess emotions (sad, happy, angry and neutral) in real time in people working with their PC through short video sessions recorded through their webcam |
| **FUNC-07** | Build a historical dataset related to stress and emotions for monitored people, which can serve for a long-term mental health assessment |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-10** | The video-based stress detection system will need to make a face detection for emotion detection. |
| **TR-P1-11** | The video-based stress detection system will use semi-supervised algorithms for data analysis. |
| **TR-P1-12** | The video-based stress detection system will provide one emotion and stress (yes/no) in almost real-time. |

***Multimodal mental health assessment based on data fusion***

*Description & System functionalities*

A long-term mental health assessment system is being developed to extract some trends of mental health in people working with their PC, by fusing historical results (stress and emotions) extracted from the video-based stress detection with online self-questionnaires launched through the Mad@Work Web App. This system performs a decision-level fusion with the above-mentioned data in order to extract relevant statistics like number of stress episodes per time, time of day when stress episodes usually occur, etc., which could be interesting for monitored people, as well as combining such data with the self-questionnaires in order to define a user pattern and extract

relevant characteristics to provide more accurate recommendations which reduce long-term stress episodes.

| Functionality ID | Description |
|---|---|
| **FUNC-08** | Assess long-term trends of mental health in people working with their PC making use of several sources of information: video sessions, physiological data and self-questionnaires results |
| **FUNC-09** | Provide personalized statistics for monitored people, such as number of stress episodes / time, time of day when stress episodes normally occur, etc. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-13** | The long-term mental health assessment system will only work correctly if video-based stress detection system provides results for the stress and emotions. |
| **TR-P1-14** | The long-term mental health assessment system will be able to process data with different time granularity |

***Recommender system***

*Description & System functionalities*

A recommender system is being developed to provide recommendations considering historical results (stress and emotions) extracted from the video-based stress detection, physiological data, results extracted from online self-questionnaires and user's preferences. Such system will be able to decide if recommendations are needed and what the most appropriate recommendations are for each person. The recommendations will be both general and specific to improve well-being, mental health or emotional level.

| Functionality ID | Description |
|---|---|
| **FUNC-10** | Provide a set of personalized activity recommendations for each monitored people which help them to mitigate stress and improve mental health. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-15** | Recommender system will generate different types of recommendations: general, wellness, mental health, emotions. |
| **TR-P1-16** | Recommender system will decide if recommendations are provided or not considering all input data related to the monitored people. |
| **TR-P1-17** | Recommender system will consider user preferences and user's feedback to the personalized recommendations |

### 3.1.4. User interaction

***Mad@Work Web App***

*Description & System functionalities*

A web app is being developed to act as an individual support tool by providing each monitored people a complete dashboard with all existing information related to the mental health and stress, as well as the management of the personalized recommendations including user's feedback.

The dashboard is being built on a data visualisation tool known as Grafana and intends to provide the monitored people much information as possible in a simple way, that is, results from the unimodal mental health assessment and the multimodal assessment, physiological data as well as a visualization of the historical data and results on a weekly, monthly and so on basis.

Additionally, the web app implements a recommendation manager able to decide which recommendations and with what priority should be offered to the monitored people according to the recommendations generated by the recommender system.

| Functionality ID | Description |
|---|---|
| **FUNC-11** | Provide a complete data visualization with much information as possible related to the mental health and stress in a simple way |
| **FUNC-12** | Manage the set of recommendations generated by the recommender system. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P1-18** | Access to the Mad@Work web app will only be done through authorization and authentication, which guarantees secure access to users. |
| **TR-P1-19** | The Mad@Work web app will provide immediate information on the level of stress and emotions to the monitored people |
| **TR-P1-20** | The Mad@Work web app will offer the option to configure user preferences in terms of viewing results and recommendations. |
| **TR-P1-21** | The Mad@Work web app will collect user feedback on the recommendations. |

## 3.2. Pilot 2 – Personalized Lighting in Indoor Work Spaces (led by Helvar)

### 3.2.1. Sensors

No sensors are used in this pilot.

### 3.2.2. Data collection

***WellTune Application***

*Description & System functionalities*

Data collection is performed through the WellTune application. When the user sets a lighting preference through the application, the hardware USB dongle is responsible for communicating with the ActiveAhead Luminaire through BLE. Once the Luminaire configuration has changed, the dongle will send a confirmation to the application. This will be recorded as a user preference.

| Functionality ID | Description |
|---|---|
| **FUNC-01** | Collect user lighting preferences with each application interaction. This includes changing the color temperature and dimming level of the luminaire. |
| **FUNC-02** | Collect user lighting preferences related to pre-defined profiles, or if the user has defined a profile by themselves. |
| **FUNC-03** | Send the data to the cloud repository with the USB dongle ID (identifies the docking station, not the user). |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P2-01** | A tunable and dimmable luminaire supporting Helvar ActiveAhead BLE protocol. |
| **TR-P2-02** | Pre-installed WellTune app on the user workstation, with access to internet. |
| **TR-P2-03** | Working USB dongle connected to the docking station. |
| **TR-P2-04** | Message containing ID, timestamp and user action sent to cloud at time of event. |

***User Self-Feedback***

*Description & System functionalities*

A separate mechanism of obtaining user feedback has not been finalised yet, it remains to be decided whether it will be integrated into the app or carried out through another medium.

| Functionality ID | Description |
|---|---|

| | |
|---|---|
| **FUNC-04** | Collect user self-feedback on productivity improvement for those who interact with the system. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P2-05** | Anonymised user feedback indicating productivity on a self-identified scale sent to cloud with timestamp and workstation ID. |

### 3.2.3. Data processing & Intelligence

***Usage Insights***

*Description & System functionalities*

The data collected for workstations would be analysed to understand how users interact with the overhead lighting control system.

| Functionality ID | Description |
|---|---|
| **FUNC-05** | Assess whether the usage frequency is adequate or not. |
| **FUNC-06** | Analyse how people modify lighting configurations (tuneable & dimmable values). For example: Is it related to time of the day, ambient conditions etc. |
| **FUNC-07** | Analyse historical patterns for seasonal variations. |
| **FUNC-08** | Analyse user feedback and determine if there is a significant impact of system usage. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P2-06** | Availability of information on the ambient conditions (outdoor natural lighting, season of the year). |
| **TR-P2-07** | Information about the previous lighting conditions to establish a baseline comparison. |
| **TR-P2-08** | Sufficient data samples have to be collected in order to reach reliable conclusions. |

### 3.2.4. User interaction

***WellTune Application***

*Description & System functionalities*

The user will primarily interact through the WellTune application and also will be given the opportunity to submit feedback. The users can view current lighting configurations and profiles in the app. However, the users will not be shown the results of the analysis. Helvar will internally evaluate the success of the system.

| Functionality ID | Description |
|---|---|
| **FUNC-09** | Users should be able to conveniently change lighting conditions through the application UI. |
| **FUNC-10** | Users should be able to provide self-feedback easily. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P2-09** | Access to WellTune app is done by collaboration with IT department, the application itself will be authorised for installation on user machines. |
| **TR-P2-10** | The self-feedback mechanism will be anonymous. |

## 3.3. Pilot 3 – Stress and performance in location independent office workers (led by FIOH & VTT)

### 3.3.1. Virtual sensors and data collection

***Computer usage logger***

*Description & System functionalities*

Logs mouse coordinates and their timestamps, events of keypresses along with the timestamp and duration, and events of application window switches along with the timestamp. Contents of keypresses and application name are not logged; for the detailed description please see pilot description above and D3.1.

| Functionality ID | Description |
|---|---|
| **FUNC-01** | Collect mouse coordinates with timestamps |
| **FUNC-02** | Collect key press events with timestamps and durations without logging key contents (except for “delete” and “backspace” keys) |

| | |
|---|---|
| **FUNC-03** | Collect window switch events with timestamps and classify each window into one of the selected categories: documents, communications etc. |
| **FUNC-04** | Ask user to verify herself and to allow data transfer |
| **FUNC-05** | Send collected data periodically to VTT server |
| **FUNC-06** | Allow user to disable data collection and/ or data transfer any time |
| **FUNC-07** | Allow user to check, modify or delete own data |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-01** | The app must work non-stop on the user computer unless the user disables it |
| **TR-P3-02** | The app must collect the above-listed data |
| **TR-P3-03** | The app must categorise keypresses into “key”, “delete” and “backspace” events and calculate event duration |
| **TR-P3-04** | The app must categorise application windows into selected window categories |
| **TR-P3-05** | The app must have an easy-to-use installer to install on users’ computers |
| **TR-P3-06** | The app must have an icon, providing access to user data folder, so that the user can see/ modify/ delete data in this folder |
| **TR-P3-07** | The app must have an icon, allowing to stop data collection or only data transfer |

***Phone data logger***

*Description & System functionalities*

This collects application categories, screen on/ off, battery level, semantic location etc.. For details, see pilot description above and D3.1.

| Functionality ID | Description |
|---|---|
| **FUNC-08** | Collect application categories, screen on/ off, battery level, semantic location etc. of the user phone. |

| | |
|---|---|
| **FUNC-09** | Sends data to VTT server |
| **FUNC-10** | Allow user to disable data collection and/ or data transfer any time |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-08** | The app works non-stop on the user phone unless the user stops it |
| **TR-P3-09** | The app stores timestamps of app switch and app category, battery level and other above-described data |
| **TR-P3-10** | The app should have UI allowing the user to stop it. |

***Self-reporting app***

*Description & System functionalities*

The app prompts the user to submit self-reports at the time moment, specified by the user, and sends the reports to VTT server. The app also has gamification feature, to maintain user interest, so the app calculates points, collected by the user, shows progress bar and other rewards.

| Functionality ID | Description |
|---|---|
| **FUNC-11** | Allow user to set the reminder time |
| **FUNC-12** | When reminder time comes, remind the user to submit the self-report |
| **FUNC-13** | Collect user answers and send the self-report to VTT server |
| **FUNC-14** | Update gamification points and levels and show them, or extra rewards, if the user earned them |
| **FUNC-15** | Allow user to modify the submitted self-report for today |
| **FUNC-16** | Allow user to submit optional self-reports for today even if self-reporting is not obligatory for today |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-11** | The app works non-stop on the computer unless the user stops it |
| **TR-P3-12** | The app has UI for customising reminder time |

| | |
|---|---|
| **TR-P3-13** | The app uses Windows notification functionality to deliver reminders |
| **TR-P3-14** | The app delivers reminders also via mobile phone and allows to set another reminder time for the phone |
| **TR-P3-15** | The app has UI to collect self-reports |
| **TR-P3-16** | The app has UI to show gamification and reasoning methods to update gamification points, levels and other rewards |

### 3.3.2. Data processing & Intelligence

***Unimodal mental condition assessment based on each data source: separate analysis of mouse data, keyboard data and app switch data***

*Description & System functionalities*

Two-class classification of users' mental conditions on monthly basis (that is, to evaluate each month as stressful or not) is the functionality required by org. barometer, because it operates on long-term conditions. We will also test stress detection on daily and weekly basis, as well as possibility to detect certain stressors from the data, e.g., interruptions.

| Functionality ID | Description |
|---|---|
| **FUNC-17** | Assess stress (yes/no) on daily, weekly and monthly basis, using each data modality separately and using self-reports and objective measures (saliva samples, cognitive tests etc.) for training and evaluation |
| **FUNC-18** | Assess potential stressors, e.g., interruptions, using each data modality separately and using self-reports and objective measures (saliva samples, cognitive tests etc.) for training and evaluation |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-17** | Each user needs to submit at least 50 self-reports for algorithm training and evaluation |
| **TR-P3-18** | Each user needs to allow data logger to run at least 4 months to collect sufficiently large set of both labelled and unlabelled data |

***Multimodal mental condition assessment***

*Description & System functionalities*

Use several modalities together: mouse, keyboard, window switch and phone data to assess mental conditions and stressors. Adapt choice of "best modalities" to each user to increase accuracy.

| Functionality ID | Description |
|---|---|
| **FUNC-19** | Assess stress (yes/no) on daily, weekly and monthly basis, using different computer data modalities together and using self-reports and objective measures (saliva samples, cognitive tests etc.) for training and evaluation |
| **FUNC-20** | Assess potential stressors, e.g., interruptions, using computer and phone data modalities together and using self-reports and objective measures (saliva samples, cognitive tests etc.) for training and evaluation |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-19** | The multimodal assessment of mental conditions and interruptions will work well only if at least one unimodal assessment module worked well. |

### 3.3.3. User interaction

***Organisational barometer***

*Description & System functionalities*

Visualises summaries (over time) of self-reports and stress detection results to individuals. Visualises summaries (over time and anonymous data of each individual) of self-reports and stress detection results to HR. The summaries include number of good and bad days, main stressors etc.

| Functionality ID | Description |
|---|---|
| **FUNC-21** | Provide visualisation of own data to each employee for self-awareness, to help to take actions for mental condition improvement. |
| **FUNC-22** | Provide visualisation of organisational unit (e.g., team) data to each employee and to the line managers, to help to take actions for improving work culture. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P3-20** | Visualisations of unit data should hide identities of individuals. |

## 3.4. Pilot 4 - Learning facility (led by Granlund)

### 3.4.1. Sensors

***IAQ IoT sensor***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-01** | Collect room air quality data, including air temperature, relative humidity, carbon dioxide, volatile organic compounds, particular matters, etc. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P4-01** | The indoor air quality device must collect data in at least few minutes frequency |
| **TR-P4-02** | Device needs to be able to send the data online continuously |

***BMS system data***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-02** | Building management system logs the HVAC system operational data |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P4-03** | The BMS data needs to be able to be accessed remotely using API |
| **TR-P4-04** | Documentation and drawings explaining BMS system functioning needs to be available while explaining each data point and measurement location |

### 3.4.2. Data collection

***Occupancy data collection***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|

| | |
|---|---|
| **FUNC-03** | Collect sample of occupancy information per room type |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P4-05** | For verification of the room occupancy estimation model, initial ground truth data collection is needed. Needed to do in one room per different ventilation type |
| **TR-P4-06** | Temporary data collection can be done using PIR sensors, occupancy camera detectors, or other. For a period of couple of days. |

### 3.4.3. Data processing & Intelligence

***Building usage and performance analytics***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-04** | Analyse building usage, its energy consumption and indoor air quality in real-time. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P4-07** | Previously mentioned sensor and data collection requirements need to be satisfied and long enough history data needs to be available. |

### 3.4.4. User interaction

***Digital Twin user interface***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-05** | 3D Digital Twin web interface for viewing and analysing building performance and is occupancy with feedback on indoor comfort. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P4-08** | 3D space model of the building is available in common format |

## 3.5. Pilot 5 - Safe to breath (led by UniqAir)

### 3.5.1. Sensors

***SmartWatcher sensor box***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-01** | IAQ (VOC, PM2.5) is measured to monitor the actual level of contaminants |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P5-01** | Power supply for measuring units. Monitoring utilizes SIM for data transfer to Server, which is located at SmartWatcher. |

### 3.5.2. Data collection

***Questionnaire to knowledge workers***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-02** | SurveyMonkey or VTT survey tool |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P5-02** | Questionnaire link to knowledge workers to give feedback either via SurveyMonkey or VTT survey tool/app |

### 3.5.3. Data processing & Intelligence

There is no data processing & intelligence in this pilot. Just manual evaluation and statistics.

### 3.5.4. User interaction

Knowledge workers give feedback via SurveyMonkey or VTT survey tool/app

## 3.6. Pilot 6 - Early Detection of Stress in the Workplace (led by Médis)

**Important Note:** *The whole pilot plan and details are dependent on the privacy and data protection analysis that is being performed by Ageas/Médis' DPO, Compliance and Legal teams, in collaboration with other partners. Pilot details might change after this analysis is finalized.*

### 3.6.1. Sensors

No sensors will be used in this pilot

### 3.6.2. Data collection

***Collection of variables through video***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-01** | Collect workers' physiological data such as perceived emotions, pupil diameter, eye gazing, eye blinking, heart rate variability and facial expressions |
| **FUNC-P6-02** | Store workers' physiological data in the data repository anonymously |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-01** | Data collection occurs according to the video-based tool usage. |
| **TR-P6-02** | The video-based tool should at least collect heart rate variability, facial expressions and eye gaze/blinking. |
| **TR-P6-03** | The software requires user to install on his/her laptop for the correct processing and storage of the data |
| **TR-P6-04** | No video recording is collected or analyzed; the only collected data are the readings of users' physiological data (perceived emotions, pupil diameter, eye gazing, eye blinking, heart rate variability and facial expressions) |

***Self-assessment questionnaires***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-03** | Collect workers' perception of their working period in terms of stress, productivity and possible reasons for their performance |
| **FUNC-P6-04** | Store workers' physiological data in the data repository anonymously |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-05** | Install an application in the user's laptop to collect questionnaire responses |

### 3.6.3. Data processing & Intelligence

***Calculation of stress level through variables collected***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-05** | Assess stress (yes/no) in real time in people working with their laptop through video feed (webcam) |
| **FUNC-P6-06** | Assess emotions (sad, happy, angry and neutral) in real time in people working with their laptop through video feed. (webcam) |
| **FUNC-P6-07** | Assess mental health in people working with their laptop in a long-term usage, through several sources of information: video feed/ physiological data and self-questionnaires results |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-06** | Each session must have:<br>- A recording plane centred on the face of the person being recorded.<br>- No appearance of other persons in the same video session. |
| **TR-P6-07** | The tool will only work correctly and be able to assess mental health status if the video-based tool correctly collects physiological data and the assessment of stress and emotions is done correctly |

| | |
|---|---|
| **TR-P6-08** | The data collected through the different sources, video and questionnaires must be uniquely identified so that they can be jointly analyzed |

***Recommendation System***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-08** | Provide a set of personalized activity recommendations for each worker for stress mitigation and mental health improvement. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-09** | Recommendation system will generate different types of recommendations: general recommendations, mindfulness, meditation, coaching, among others. |

### 3.6.4. User interaction

***Individual tool***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-09** | Provide personalized statistics for workers such as number of stress episodes / time, time of day when stress episodes normally occur, etc. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-10** | Access to the individual tool will only be done through authorization and authentication, which guarantees secure access to users |
| **TR-P6-11** | The individual tool will offer the option to configure user preferences in terms of viewing results and recommendations |
| **TR-P6-12** | The individual tool will collect user feedback on the recommendations made. |

***Organizational barometer***

*Description & System functionalities*

| Functionality ID | Description |
|---|---|
| **FUNC-P6-10** | Provide team leaders/managers aggregated anonymized data regarding stress levels of the whole team |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P6-13** | Data provided and presented has to be anonymized and aggregated, so that no individual person can be identified by the managers |

## 3.7. Pilot 7 - Pilot *WellMind* (led by ETRI)

### 3.7.1. Sensors

***Smart Watch***

*Description & System functionalities*

Physiological data can be collected through Samsung Watch, a wearable device that provides heart rate and IBI(Inter-Beat Interval).

| Functionality ID | Description |
|---|---|
| **FUNC-01** | Collect workers' physiological data such as heart rate, Inter-Beat Interval using PPG sensors |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P7-SW-001** | The wearable device should be able to collect physiological data (e.g., heart rate, Inter-Beat Interval). |

***Environment Sensor Device (ESD)***

*Description & System functionalities*

This component collects environmental data, including sound, noise, temperature, humidity, distance, and air quality. The device periodically passes data to the app via USB or BLE communication.

| Functionality ID | Description |
|---|---|
| **FUNC-02** | Collect working environmental data such as temperature, humidity, noise, CO2 and movement |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P7-ESD-001** | The device should be able to collect the working environmental data (temperature, humidity, noise, CO2, movement, etc.). |

### 3.7.2. Data collection

***Mental Health Collection (MHC)***

*Description & System functionalities*

This Component periodically collects workers' physiological data, environmental information and schedule information. The questionnaire information is collected by app surveys according to the situation of knowledge workers. The questionnaire can be composed of a profile questionnaire that you only need to answer once, job stresses that users respond periodically, and general stress questionnaire. The collected data is stored in Database.

| Functionality ID | Description |
|---|---|
| **FUNC-03** | Collect and store workers' survey data, physiological data, environmental data, and work-related schedules |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P7-MHC-001** | The system should provide a function that enables users to take a survey on a regular basis during their working hours. |
| **TR- P7-MHC-002** | The system should provide a function that enables users to take a daily survey during working hours before they leave the office. |
| **TR- P7-MHC-003** | The system should be able to collect and store physiological data (e.g., heart rate, Inter-Beat Interval). |
| **TR- P7-MHC-004** | The system should be able to collect and store the working environmental data (temperature, humidity, noise, CO2, movement, etc.). |
| **TR- P7-MHC-005** | The system should be able to collect and save the data of work-related schedules. |

***User Information Management (UIM)***

*Description & System functionalities*

This Component performs functions such as registering user information using the system, registering a role that can distinguish whether a user is a manager or a knowledge worker, registering a worker's department, and managing data access rights.

| Functionality ID | Description |
|---|---|
| **FUNC-04** | Manages user and organization registration, and data access authorization |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P7-UIM-001** | The system should provide a function to add/edit/delete users in an organization. |
| **TR- P7-UIM-002** | The system should provide a function to register/edit/delete users. |
| **TR- P7-UIM-003** | The system should provide a function to register/edit/delete the role of the users. |
| **TR- P7-UIM-004** | The system should provide a function to register/edit/delete an organization. |
| **TR- P7-UIM-005** | The system should provide a function to manage authority to access data according to user/role/organization. |

### 3.7.3. Data Processing & Intelligence

***Mental Health Analysis and Assessment (MHA)***

*Description & System functionalities*

This component provides AI-based methods for mental health analysis and assessment. The component detects the stress state by the mental health index, which is based on multiple source data fusion and calculated by adding static mental health index, dynamic mental health index, and task load index.

| Functionality ID | Description |
|---|---|
| **FUNC-05** | Detects the stress state by the mental health index |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR-P7-MHA-001** | The system should be able to analyse the integrated stress index. |
| **TR- P7-MHA-002** | The system should be able to analyse detailed stress data (e.g., survey questionnaires, schedule, working environment status, physiological index, etc.). |
| **TR- P7-MHA-003** | The system should provide a function to analyse the stress status information by a specific period (e.g., a day, a week, a month).<br>* Examples of the stress status information: subjective stress status, physiological stress index, energy index, the number of clicks on the stress button, etc. |
| **TR- P7-MHA-004** | The system should be able to analyse and predict the stress of the day. |

***Well-Being Effectiveness Analysis (WEA)***

*Description & System functionalities*

This component measures the effect of a well-being solution performed by a knowledge worker to relieve stress, and can provide a visualization of the stress-relieving effect. Knowledge workers may not accept the well-being solution recommended by the system due to work schedules, etc. The system should be able to manage historical information about wellness solutions used by knowledge workers.

| Functionality ID | Description |
|---|---|
| **FUNC-06** | Offers a stress-relief effectiveness after experiencing the solution |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR- P7-WEA-001** | The system should be able to measure the stress relief effectiveness of the solution (e.g., by measuring physiological signal for five minutes or conducting a survey about the level of satisfaction). |
| **TR- P7-WEA-002** | The system should be able to display the stress relief effectiveness. |
| **TR- P7-WEA-003** | The system should be able to detect and process users' refusal to use the solution. |
| **TR- P7-WEA-004** | If users do not accept the solution, the system should allow users to skip the measurement of the stress relief effectiveness. |
| **TR- P7-WEA-005** | The system should be able to manage and display the information about the solution that users previously used. |

### 3.7.4. User interaction

***Mental Health Information Display***

*Description & System functionalities*

This component should be able to analyse the stress state to display a comprehensive and detailed stress state (e.g., survey questionnaire, schedule, work environment state, physiological state, etc.). The component should also be able to provide a stress notification to the user when stress is detected. When the user wants to check the history of stress data, the system should provide a function to inquire it. If knowledge workers exceed the threshold of stress, the system should provide the ability to guide well-being solutions.

| Functionality ID | Description |
|---|---|
| **FUNC-07** | Display the working environment information, physiological data, and detailed stress data. |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR- P7-HID-001** | The system should be able to display physiological data (e.g., heart rate, HRV Analysis Information). |
| **TR- P7-HID-002** | The system should be able to display the working environment data (temperature, humidity, noise, CO2, movement, etc.). |
| **TR- P7-HID-003** | The system should be able to display the integrated stress index. |
| **TR- P7-HID-004** | The system should be able to display detailed stress data (e.g., survey questionnaire, schedule, working environment index, physiological index, etc.). |
| **TR- P7-HID-005** | The system should provide a function to send a notification when stress is detected. |

| | |
|---|---|
| **TR- P7-HID-006** | The system should provide a function to display the stress data to inform users of the stress situation. |
| **TR- P7-HID-007** | The system should be able to display on the monitoring board the stress status related to the information that they input most recently in the self-report. (e.g., the status of stress and energy). |
| **TR- P7-HID-008** | The system should provide a function to display the stress status information by a specific period (e.g., a day, a week, a month). * Examples of the stress status information: subjective stress index, physiological stress status, energy index, the number of clicks on the stress button, etc. |
| **TR- P7-HID-009** | The system should be able to provide the visualised analysis results of stress data. |
| **TR- P7-HID-010** | The system should provide a function for checking the history of members' stress data. |
| **TR- P7-HID-011** | The system should provide a function for checking the stress relieving guide for members. |
| **TR- P7-HID-012** | The system may provide a function to inform task managers with user's consent when the stress level of members surpasses the threshold (via email, text message, pop-up, etc.). |
| **TR- P7-HID-013** | The system should be able to display the daily schedule and estimation of the stress of the day on the screen. |

***Mental Well-Being Support (MWS)***

*Description & System functionalities*

This component must provide a function that allows the user to edit the encouraging phrase displayed on the display device according to his or her preference. The component should also provide the ability for users to enter the type of wellbeing solution they prefer, and automatically display a wellbeing solution when it detects a stressful state.

| Functionality ID | Description |
|---|---|
| **FUNC-08** | Offers a tailored well-being solution |

*Technical requirements*

| Tech Req ID | Description |
|---|---|
| **TR- P7-MWS-001** | The system should provide a function that allows users to edit complimentary comments according to their preferences. |
| **TR- P7-MWS-002** | The system should be able to display complimentary comments at all times. |
| **TR- P7-MWS-003** | The system should provide a function that allows users to set up the type of stress relief solution based on user's preferences. |
| **TR- P7-MWS-004** | The system may display a stress relief solution automatically, considering long hours of sitting, consistent stress, or continuous alerts for environment data. |
| **TR- P7-MWS-005** | The system should allow users to input whether or not they have used the solution. |

# 4. Ethically Aligned Design

## 4.1. Trustworthy AI – EU Ethics guidelines for trustworthy AI

High-Level Expert Group on Artificial Intelligence (AI HLEG) – an independent expert group – was set up by the European Commission in June 2018 in order to craft guidelines to promote and set out a framework for achieving Trustworthy AI. This work produced a document "Ethics Guidelines for Trustworthy AI", made public on 8 April 2019, that identifies three components for the AI system to meet throughout its entire life cycle in order to be considered trustworthy:

1. ***lawful:*** *complying with all applicable laws and regulations,*
2. ***ethical:*** *ensuring adherence to ethical principles and values, and*
3. ***robust:*** *both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm.*

   (AI HLEG, 2019)

*Ethics guidelines for Trustworthy AI* aims to offer guidance towards achieving the latter two components of Trustworthy AI: ethical and robust AI and does not explicitly deal with the first component: lawful AI. However, it is pointed out that law provides both positive and negative obligations: what should be done, and what may be done, and for **lawful AI**, the system needs to be developed in accordance with any legally binding rules or regulations. The relation between legislation and the Ethics Guidelines for Trustworthy AI is stated and limited in the document as follows: *"These statements are not meant to provide legal advice or to offer guidance on compliance with applicable laws, though it is acknowledged that many of these statements are to some extent already reflected in existing laws"*, and with more explicit notion: *"Nothing in this document shall be construed or interpreted as providing legal advice or guidance concerning how compliance with any applicable existing legal norms and requirements can be achieved. Nothing in this document shall create legal rights nor impose legal obligations towards third parties."* (AI HLEG, 2019)

In the document by AI HLEG (2019) a concern is raised on laws sometimes lagging on technological advancements, such as artificial intelligence, or that laws may not be suited to address certain issues regarding them. Additional concern regarding legislation that is pointed out, is that it sometimes may be *"out of step with ethical norms"* when dealing with new technologies. Hence, in addition to the requirement of AI being lawful, it is suggested that AI systems should align with **ethical** norms. Four ethical principles are introduced, that should be adhered to when developing, deploying, and using AI: *respect for human autonomy, prevention of harm, fairness,* and *explicability* – that stem from human and citizen's rights, individual freedom, respect for democracy, justice and law, equality, non-discrimination, and solidarity.

Ethical and **robust AI** are stated in the AI HLEG (2019) document to be closely intertwined and to complement each other. Robust AI system should induce confidence of not causing unintentional harm, be safeguarded against unintended adverse impacts, and to function in a *"safe and secure manner"*. Robustness of the system is needed and expected from both technical and social perspectives.

In addition to the three components (lawful, ethical, and robust AI), seven (7) key requirements from systemic, individual and societal aspects are set for all AI systems to meet and to be in place:

1. *human agency and oversight,*
2. *technical robustness and safety,*
3. *privacy and data governance,*
4. *transparency,*
5. *diversity, non-discrimination and fairness,*
6. *environmental and societal well-being, and*
7. *Accountability.*

(AI HLEG, 2019)

**Reference:** AI HLEG: Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. (2019). "Ethics Guidelines for Trustworthy AI". https://doi.org/10.2759/346720

## 4.2. ECCOLA – a Method for Implementing Ethically Aligned AI Systems

Following AI-related technological progress, the discussion on the field of AI ethics has seen a vast increase during the past decade. This dialogue has resulted in a set of key principles that cover a wide range of subjects – such as demand for explainable AI systems that are aligned with human rights and well-being – and are now widely acknowledged as central issues in AI ethics. Transferring this discussion into practice and actually influencing the development of AI systems has thus far been a problem, that has mostly been treated with either laws and regulations or guidelines devised by companies, governments and standardization organizations – such as the *Ethics guidelines for Trustworthy AI* introduced in the previous chapter.

Despite the efforts and active discussion, the research on AI ethics has been largely theoretical and conceptual with a focus on defining key principles and how to tackle them – yet leaving a prominent gap between research and practice. Numerous guidelines for AI ethics have tried to bridge this gap, but have not been very successful in bringing these principles to developers, and have left developers struggling with how to implement the widely abstract ethical guidelines into development processes. Indeed, past research has shown that guidelines are rarely effective in software engineering. *ECCOLA – a Method for Implementing Ethically Aligned AI Systems* was developed to bridge this gap with another approach.

In the Mad@Work project, ECCOLA is used in all the pilots, in order to ensure that ethical considerations have been implemented throughout the design, development and deployment of the AI solution. ECCOLA is a modular, sprint-by-sprint process designed to facilitate ethical thinking in AI/S (Artificial Intelligence/Autonomous System) development, and designed to be used together with existing methods. It takes on the form of a deck of 21 cards, split into 8 AI ethics themes (e.g., transparency), with each theme consisting of 1 to 6 cards. From the get-go, ECCOLA was never intended to be a stand-alone method, but rather, a modular extension to existing software development methods that would provide developers an actionable tool for implementing AI ethics into the process. So far efforts on creating ethical machine learning technologies have focused on the “what”, whereas ECCOLA has focus set on the “how” of AI ethics. ECCOLA does not provide any direct answers to ethical problems, as arguably correct answers are a rare breed in ethics in general, but rather asks questions in order to make the organization consider the various ethical issues present in AI systems. In developing ECCOLA, three main goals for the method were set:

1. To help create awareness of AI ethics and its importance,
2. To make a modular method suitable for a wide variety of SE contexts, and
3. To make ECCOLA suitable for agile development, while also helping make ethics a part of agile development in general.

ECCOLA is built on AI ethics research and utilizes both existing theoretical and conceptual research, as well as AI ethics guidelines that have been devised based on existing research as well. In terms of guidelines, the cards are based primarily on the IEEE Ethically Aligned Design guidelines and the EU Trustworthy AI guidelines. The eight (8) AI ethics themes covered in the cards are: *analyze, transparency, safety and security, fairness, data, agency and oversight, wellbeing,* and *accountability*. Each card in ECCOLA is split into three parts: (1) motivation (i.e., why this is important), (2) what to do (to tackle this issue), and (3) a practical example of the topic (to make the issues more tangible).

ECCOLA supports iterative development. During each iteration, the team is to choose which cards, or themes, are relevant for that particular iteration. ECCOLA is intended to be used during the entire design and development process in a three step process that is repeated in every iteration. (1) Prepare: Choose the relevant cards for the current sprint. (2) Review: Keep the selected cards on hand during work tasks. Write down on the cards the actions you have taken and (ethical) discussions you have had. (3) Evaluate: Review to ensure that all the planned actions were taken. Revise the card deck as needed, and repeat the process. Remember to do a retrospective afterwards. ECCOLA is also method-agnostic, making it possible to utilize it with any existing or in-house SE method, which is one of the major reasons for selecting ECCOLA to be used in the Mad@Work project and its diverse in nature pilots.

**References and resources for ECCOLA:**

V. Vakkuri, K.-K. Kemell, M. Jantunen et al., ECCOLA - a method for implementing ethically aligned AI systems. The Journal of Systems & Software (2021), doi: https://doi.org/10.1016/j.jss.2021.111067

Vakkuri, Ville; Kemell, Kai-Kristian; Abrahamsson, Pekka (2020): Internet resource for ECCOLA - a Method for Implementing Ethically Aligned AI Systems. figshare. Poster. https://doi.org/10.6084/m9.figshare.12136308.v2

# 5. Privacy guidelines/requirements

## 5.1. Data protection by design guidelines

See Appendix 3: Data protection by design guidelines for the full guidelines for each scenario.

**Scenario 1 - the solution is for the use of an employer.** The employer (company) will be the data controller. The Description column includes guidance that often falls on the data controller's area of responsibility. However, the solution designer can do their part. The solution designer should ensure that the solution supports the controller's responsibilities and mitigates risks that can be foreseen. Guidance for this case is given in the Scenario 1 column.

**Scenario 2 - the solution is for the sole use of an individual.** The solution provider should refer to the Description column directly. Some specific guidance is included.

**Solution provider's own use of data -** In both scenarios, if the solution provider uses any of the personal data (e.g. a person's usage data) for product improvement, analytics etc, the solution provider is a **data controller** for that data use case and should refer to the Description column directly.

**Solution provider provides a service for the company -** if in Scenario 1 the solution provider offers ongoing product support and maintenance service, analytics services, data storage for the data in the solution etc, they will be a **data processor** for the company.

## 5.2. Common threat model

This threat model contains common privacy and data protection threats for a Mad@Work type of a solution when it is in use. The model is generic and can be used when modelling threats in specific solutions.

**Terms used**

Note: this terminology mirrors that of security threats, where terms attack point, attack vector and security threat are used.

- **Who can be harmed - Data subject:** Data subject is the individual whose data is processed. They are **the "protected asset"** whose privacy and personal data has to be safeguarded by the data controllers. Failure to do these damages the data subject as well as puts the controller (and potentially the processor too) at a risk of data protection authority sanctions.
- **Where harm can happen - Vulnerable points**: points that are vulnerable to privacy and data protection (non-compliance) threats.
- **How harm can happen - Harm vectors**: path, scenario or means through which privacy or compliance is harmed.
- **What can happen - Threats**: issues arising from personal data processing that can cause damage data subjects' right to privacy and data protection (non-compliance) or have a negative impact on data subjects
- **What are the consequences - Harm:** impact on data subjects and to their right to privacy and compliant processing of their data

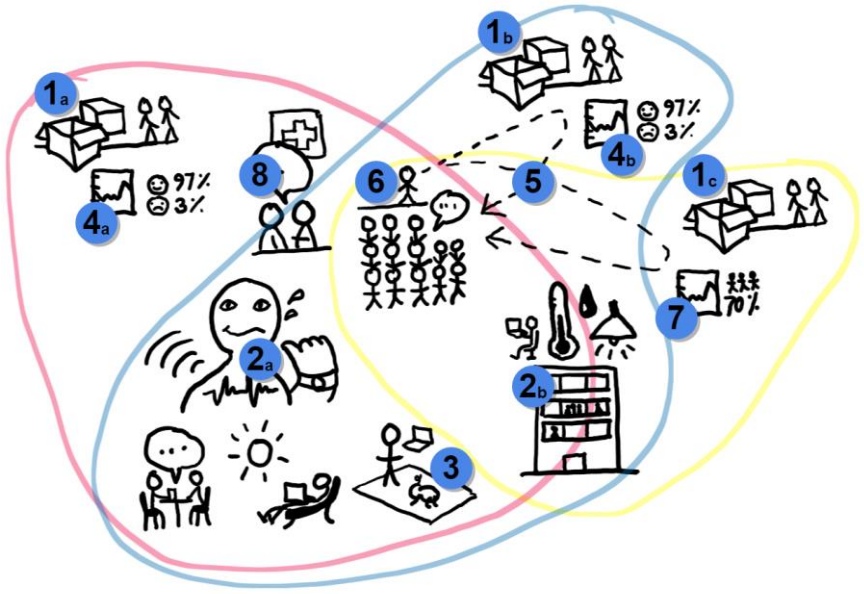



*Figure 9 - Visual generic privacy and data protection threat model for Mad@Work solutions*

- Red: Potential reach of data processing for personal wellness solution
- Blue: Potential reach of data processing for employer/HR use
- Yellow: Potential reach of data processing for work environment optimisation

| ID | Vulnerable points | Threats |
|---|---|---|
| 1a-c | New innovative technology | • Unknown compliance, ethical and social consequences, negative consequences<br>  ○ Intentionally/unintentionally created new personal data and processing activity that is not legal<br>  ○ Non-personal data turns personal data<br>  ○ Unexpected impact to data subjects<br>• No ethical framework or regulation that fits<br>• Difficult to explain to data subjects |
| 2a-b | Data capture | • Poorly defined and managed personal data<br>  ○ Personal data not recognised as such<br>  ○ Sensitive data not recognised as such<br>  ○ Data controllership for captured data unclear<br>  ○ No legal basis for capturing personal data<br>  ○ No legal basis for capturing sensitive personal data<br>  ▪ Explicit consent<br>• Poor quality data / data contamination |

| ID | Vulnerable points | Threats |
|---|---|---|
| | | ○ Capture context is difficult to control<br>○ Data captured from work and home life situations/tasks due to the breath of context<br>○ Data captured of other people or mixes up with data subject data (colleagues, family, friends)<br>○ Poorly defined data capture not lawful<br>• Degree of anonymisation not high enough for the context<br>○ Anonymisation performed late in the process (i.e. not at the source)<br>○ At some point of processing someone can single out individuals<br>○ Additional information held by someone can be used to identify people<br>○ Information of a person can be inferred from a group membership (i.e. "all employees under 25 are stressed" - my 20-year old colleague is stressed)<br>○ Changes in sample weaken anonymisation / make data identifiable<br>▪ team size changes, holidays, tasks and habits, demographics<br>○ Digital phenotypes/digital "fingerprints" allow linkability of records and potential identification |
| 3 | Data subject position | • Data subject poorly informed<br>○ Too complex to explain<br>• Data subject lacks control of the processing, lacks autonomy<br>○ Data capture: Where, what, how and when<br>○ Data use purposes: Who and why<br>• Consents not valid<br>○ Informing data subjects not comprehensive enough<br>○ Consent cannot be given freely / There is a power imbalance<br>○ Easy withdrawal of consent not possible<br>• Solution considered invasive<br>○ Data collection methods<br>○ Analysis reveals too much<br>○ No chance of self-regulation or setting privacy boundaries (inner emotions revealed)<br>• Unintended impact on health |

| ID | Vulnerable points | Threats |
|---|---|---|
| | | ○ Solution reveals a hidden health issue unknown to data subject<br>○ Solution aggravates a health condition<br>• Solution not equipped to dealt with change in data subject status/situation<br>○ Data subject turns vulnerable / becomes ill<br>○ Employment status or position changes |
| 4 | Data in solution provider's possession/reach | • Solution provider has a processor role without data processing agreement in place<br>• Solution provider has a controller role (Data used for provider's own purposes) but no legal basis for viewing/storing/using (=processing) that data<br>○ Contract, legitimate interest, consent, explicit consent?<br>○ Developing this and other services/products, providing other services/products, marketing, selling data, profiling persons etc<br>• Poor security measures |
| 5 | Data in employer's possession/reach | • No legal basis for data processing / Data processing not lawful under national or sector legislation<br>○ Consent cannot be freely given<br>○ Legitimate interest not balanced<br>○ No legal requirement to collect data<br>○ Not necessary for employment contract<br>○ Data collection specifically regulated and not lawful<br>• Analyses and actions based on analyses<br>○ Analyses are used to make changes that impact employees negatively<br>○ Analyses are used to make changes that unfairly disadvantage certain groups (intended/not intended)<br>○ Individuals' home life circumstances distort the analyses and subsequent actions affect the workforce<br>• Several solutions' data combined<br>○ New information about data subjects is generated (intentionally or unintentionally)<br>○ No legal basis for combining data<br>• Access to data not strictly managed and minimised<br>○ Employees, managers, IT |

| ID | Vulnerable points | Threats |
|---|---|---|
| 6 | Employer sponsoring the solution | • Employer has interest in/expectations regarding employees' use of the solution<br>• Employer transfers its responsibilities relating to employee wellbeing to the employee<br>• Employees spontaneously share the results with employer to influence decisionmaking (e.g. requests for lessening one's workload)<br>• Employer informally asks for the results to support decisionmaking (e.g. to support promotion)<br>• Teams/colleagues expect colleagues to share results informally for team, resourcing and support purposes (social pressure for sharing) |
| 7 | Data for work environment optimisation | • Personal data not recognised as such<br>• Degree of anonymisation not high enough for the context<br>  ○ Non-personal data becomes personal data unintentionally<br>  ○ Other threats (see anonymisation) |
| 8 | Data used in healthcare | • Data controllership unclear<br>• Ethics, legality and regulation of processing unclear |

## 5.3. Threat catalogue

This threat catalogue should be read in conjunction with the visual threat model above.

### 5.3.1. Theme: Controllership and legality of processing

***Description***

Unclear controllership and poor analysis and documentation can lead to parts of personal data protection being overlooked.

All personal data has to have a named data controller (or named joint controllers). All processing activities must be lawful in general, as well as have a selected basis for processing from those listed in the GDPR. National and sector legislation governing personal data processing should be taken into account.

***Potential consequences***

- Non-compliance: Processing is not legal (incl. collection, storage, use, reuse, anonymisation, deletion)
- Harm to data subject: Poorly managed data may leak, get misused, destroyed, inappropriately viewed or processed. Data subject's fundamental rights to privacy and data protection may be breached.

***Harm vectors and controls***

| Harm vector | Potential controls |
|---|---|
| Poor understanding and documentation of data types, processing activities, legal basis and controllership. | • Document all processing (data and system inventories, record of processing activities).<br>• Have data processing agreements in place between controllers and processors. |
| Data capture poorly managed | • Plan the lifecycle of all data captured<br>• Plan carefully how the GDPR principles are implemented in all data capture - control legality by strict adherence to the principles (minimisation, accuracy, purpose specification etc.) |
| Data for employer use | • Map all relevant legislation and its impact on the processing (e.g. legislation relating to privacy at workplace, legislation relating to sector)<br>• Document the legal basis for all activities done on the personal data |
| Data in solution provider's possession/reach | • Document what processing is done as a processor and what as a controller<br>• Document the legal basis for all activities done on the personal data<br>• Provide transparent documentation about processing<br>  ○ if controller: directly to data subject<br>  ○ if processor: to the controller<br>• Have data processing agreements in place for all controller-processor relationships |
| Data for work environment optimisation | • Carefully assess whether the data is at any point, or has potential to become, personal data or sensitive personal data.<br>• Plan anonymisation carefully and fit it to the context<br>  ○ Follow reputable anonymisation guidance<br>  ○ Stay up to date of the state of art<br>  ○ Recognise anonymisation as a processing activity performed on personal data - and have a legal basis for it |
| Data used in healthcare | • Carefully plan healthcare role in the solution, taking into account any restrictions stated in relevant legislation and |

| Harm vector | Potential controls |
|---|---|
| | the interests of all the parties (employer, employee, healthcare provider) |

### 5.3.2. Theme: Data and data capture methods

***Description***

When unordinary data types are collected via unordinary methods and further analysed and combined, it can be difficult to assess whether the data is personal data, or even sensitive personal data. The same data type can be sensitive in one context and non-sensitive or not even personal data in another. New highly sensitive data types may not listed and recognised as such in the current regulation, guidance or ethical frameworks. Therefore all data types need to be assessed in time and context and their sensitivity set accordingly. Anonymisation and pseudonymisation techniques as well as techniques for breaching these develop constantly, and risk-free anonymisation can rarely be achieved in complex data-rich solutions. The level of risk helps to point the acceptable degree of anonymisation.

***Potential consequences***

- Harm to data subject: Data subject's right to privacy is harmed - sensitive data leaks
- Non-compliance: Sensitive data is processed unlawfully and insecurely

***Harm vectors and mitigations***

| Harm vector | Potential controls |
|---|---|
| Data capture management | • Carefully assess whether the data is, or has potential to become, personal data or sensitive personal data.<br>  ○ Plan for the data lifecycle<br>• Ensure that data is captured according to GDPR principles (minimisation, accuracy, purpose specification etc.)<br>• Ensure that all captured data has a data controller.<br>• Ensure that all purposes for the captured data are known. Anticipate and control further re-use. |
| Anonymisation methods | • Follow reputable anonymisation and pseudonymisation guidance<br>• Stay up to date of the state of art |

### 5.3.3. Theme: New innovative technology

***Description***

New innovative technology may have unintended undesirable consequences. It may not be well regulated yet and can lack guidance and ethical framework. Compliance may be difficult to prove. Traditional assessment methods may not be able to uncover emergent threats.

***Potential consequences***

- Harm to data subject: unknown / unknowable
- Non-compliance: uncertain

***Harm vectors and mitigations***

| Harm vector | Potential controls |
|---|---|
| Technology is new and innovative | • Wide modelling and thorough impact assessment that assesses harm to people, with the technology assessed in its wider context, with people and ethical issues taken into account<br>• Ongoing monitoring for unintended consequences |
| Combination of technologies and solutions | • Assessment of impact for the combined solution<br>• Ongoing monitoring for unintended consequences<br>  ○ Emerging new processing activity<br>  ○ Emerging new personal data<br>  ○ Non-personal data turning into personal data |

### 5.3.4. Theme: People and context

***Description***

People and context are the less controllable elements. New threats and harms can emerge when the solution is targeted for different people and different contexts.

***Potential consequences***

- Harm to data subject: Type and level of harm is dependent of the person's situation
- Non-compliance: Specific requirements for different contexts are overlooked (e.g. sector specific legislation)

***Harm vectors and mitigations***

| Harm vector | Potential controls |
|---|---|
| People do not only work in offices and during office times | • Setting solution to measure only at certain locations, times, tasks etc<br>• Increasing people's autonomy and control of the solution<br>  ○ Data capture: Where, what, how and when - what should count<br>  ○ Data use purposes: For whose use and why |

| Harm vector | Potential controls |
|---|---|
| People's wellbeing is a sum of work and non-work related aspects | • Increasing people's autonomy and control of the solution<br>  ○ Data capture: Where, what, how and when - what should count<br>  ○ Data use purposes: For whose use and why<br>  ○ Challenging automatic results (e.g. marking discrepancies between how they feel vs. results given by the solution) |
| Context is not static | • Technical controls and adjustments<br>  ○ Ability to adjust data capture depth and breadth (e.g. accuracy, anonymisation measures, who to target)<br>  ○ Ability to adjust analysis & reporting depth and breadth<br>• Ongoing monitoring of the context<br>  ○ Team make up and size, changing tasks and roles, people's situations<br>  ○ Building use and layout |

## 5.4. GDPR consent in research

*This guidance has been written from the EU GDPR perspective. The word "consent" has a specific meaning in the GDPR. In the GDPR, consent refers to specifically to consent for personal data processing, which is not the same as consent to participate in research, for example. Consent is one of the legal bases under which personal data may be processed and for it to be valid, the strict rules of GDPR consent must be followed. Please note that when the purpose of personal data processing is research, GDPR offers a number of exceptions to the general rules. Therefore, this guidance should only be read in the context of research.*

### 5.4.1. Consent as a legal basis

This guidance assumes that consent has been chosen as the legal basis for processing research participant data. Consent is only one of the available legal bases for personal data processing. Instead of using consent, the participants could for example be asked to enter a contract. Using consent means that the data subject must be totally free to agree to it and also totally free withdraw it whenever they wish. If this cannot be guaranteed in practice, other legal bases should be considered. Legitimate interest or contract may be available to use.

If consent is used, for it to be valid, it has to follow the strict requirements set in the GDPR. It has to be freely given and it must not be asked in a pressured situation or an unbalanced context. For example, an employer asking an employee to consent is generally not accepted as a valid consent, since the employee is in a weaker position in relation to their employer.

It is important to note that research participation consent (See section in informed consent) is not the same as GDPR consent for personal data processing. These are two distinct consents that can exist at the same time. This guidance applies only to the latter.

It should also be noted that GDPR consent cannot be used to make whatever data collection lawful as long as people consent. GDPR principles of minimising data, fairness etc must still be followed.

- GDPR consent should be recognised as one possible legal basis for personal data processing and chosen if it is appropriate. It cannot be later swapped to another basis.
- Processing under GDPR consent must be designed carefully.

### 5.4.2. Freely given consent

The GDPR requires that consent is freely given. It means that the data subject must have a free choice, must not feel pressured to consent and should not get negative consequences from not consenting. Consent text must be presented separately from terms and conditions and other such parts/sections that the data subject has to agree to.

### 5.4.3. Purposes of personal data processing

The GDPR requires personal data processing purposes to be set in advance and communicated to the data subjects. This is usually done via a privacy notice. While the consent text should be clear on what purposes the data subject is agreeing to, not all of the information from the privacy notice need to be repeated in the consent text.

- The GDPR consent text must state what specific purposes the data is to be processed for.

### 5.4.4. "Research purposes"

The GDPR includes some special allowances when the personal data is used for research. "Research" is interpreted broadly, and can include for example technological development and demonstration, fundamental research, applied research and privately funded research. European Data Protection Board (EDPB) guidance adds that the research project set up is expected to be in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.

Defining the specific purposes for personal data in advance may be challenging in research, but it must not be ignored. GDPR recital 33 addresses this by stating the following. "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research (note: rather than consenting to using the data for a certain purpose) when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." The EDPB adds that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.

The EDPB suggests

- The GDPR consent text should aim to define at least the area of research.

### 5.4.5. "Statistical purposes"

The GDPR includes some special allowances when the personal data is used for statistical purposes. The research may involve collecting personal data and then turning that into statistical data. In the GDPR "statistical purposes" implies that the resulting data is aggregated, anonymous data, and that the created statistical data (or the original personal data) is not used in support of measures or decisions regarding any particular person. Statistical purposes also include statistical surveys and the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose.

- If the GDPR consent text refers to statistical purposes as a personal data use case, please note this interpretation.

### 5.4.6. Further processing

Once the research project has finished, the researchers might want to use the personal data for other projects as well, or, the researchers may wish other research to benefit from the data too.

- These further purposes should also be mentioned on the consent text.

### 5.4.7. Processing of special category data (e.g., health data)

Processing of special category data, such as health data, is generally prohibited. GDPR offers a few exceptions to this rule. It is lawful if the data subject gives an explicit consent. Explicit consent differs from ordinary consent and should be asked separately. It must be worded especially clearly so that the person can be certain how their special category data is used. Explicit consent must be expressly agreed to, for example by a signature or ticking a separate tick box.

- If special category data is collected, the consent must be "explicit".

### 5.4.8. Anonymisation and deletion

Please note that anonymisation and deletion are processing activities, and all processing done to the personal data should be covered by the consent, unless another legal basis is used to cover those processing purposes (for example, if it is a legal requirement to anonymise research data for re-use).

- If the collected data is to be anonymised or deleted, the consent should cover that as well.

### 5.4.9. Record of consent

It is important to keep records of all consents and whether someone has withdrawn their consent. If tick boxes are used, a time stamp and the person's identity should be recorded alongside. A signature is not necessary, if the consent can otherwise be reliably recorded. Digitally recorded consent can be easier to manage.

### 5.4.10. Withdrawal of consent (Right to be forgotten)

The data subjects should be able to withdraw their GDPR consent as easily as they gave it. If they withdraw their consent, their data should be deleted. The data needs to be organised in a way that makes possible accommodating these kinds of requests, e.g., naming data sets in a certain way. The data controller should ask all parties to whom it has disclosed the data to delete the data as well.

The EDPB notes that while withdrawal of consent could undermine types of scientific research that require data that can be linked to individuals, the GDPR is clear that consent can be withdrawn, and controllers must act upon this – there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research. I.e. personal data is anonymised and non-personal data retained.

However, if the research in question is scientific research (rather than private/commercial) and the deletion of that person's data would seriously jeopardise the achievement of the research objectives, the data controller could state that the personal data is necessary to retain and cannot be deleted. This is allowed by GDPR Article 17(3)(d).

#### 5.4.11. GDPR references

Relevant GDPR articles and recitals regarding consent and research.

- Article 7, Conditions for consent
- Article 89, Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- Recital 159, Processing for Scientific Research Purposes
- Recital 157, Information from Registries and Scientific Research
- Recital 156, Processing for Archiving, Scientific or Historical Research or Statistical Purposes
- Recital 162, Processing for Statistical Purposes
- Recital 33, Consent to Certain Areas of Scientific Research
- Recital 65, Right of Rectification and Erasure
- Recital 62, Exceptions to the Obligation to Provide Information

Relevant EU-level guidance:

- Guidelines 05/2020 on consent under Regulation 2016/679

### 5.5. Examples of GDPR consent

#### 5.5.1. General guidelines

- Check that consent is the legal basis that is the most appropriate one for your case.
- Make sure that the consent can be freely given. Remove any pressure and conflicting interests from the situation. Only freely given consent is valid.
- Ask GDPR consent separately from everything else - particularly separate from research participation consent and other approval/agreement points.
- Make sure that the wording is very clear to the participants, and it covers everything you are planning to do with the data. You may refer to the research plan and privacy notice.
- Keep a record of consent: who gave it, for what, and when. The record can be digital.

- Do not use pre-ticked boxes or opt-outs. The data subject must carry out the action to consent themselves.
- Offer an easy consent withdrawal mechanism. Make sure you have a system for processing any consent withdrawals, including informing all parties to whom you have disclosed the data.

### 5.5.2. Sample consent – VALID

> [ ] *I consent to my personal data to be processed for research in the areas of health, wellbeing and employment, in line with the privacy notice (link/attached).*
>
> *More information about this research project can be found on the information sheet.*
>
> *You can withdraw your consent at any time by emailing researchconsent@researchproject.com.*

THIS IS VALID FOR GDPR CONSENT

- The consent concerns specifically the use of personal data
- Date stamp and identity of person are captured, which creates a record of consent (alternatively, ask for a signature & date)
- No special category data is collected, so no explicit consent is needed
- A privacy notice is available to review, which states the purposes, all collected categories of personal data, what is done with the data afterwards etc.
- The person is told about consent withdrawal, and it is made easy

### 5.5.3. Sample explicit consent - VALID

> *Consent for personal data & special category personal data processing*
>
> *I consent to my personal data to be processed for research in the areas of health, wellbeing and employment, in line with the privacy notice (link/attached). More information about this particular project can be found on the information sheet.*
>
> *Health data: We would collect information of your general mental and physical health including what long term illnesses you have and what medication you take. This health data is used for understanding your level of health and finding correlations between your physical and mental stress markers. Once the research project is over, all data will be anonymised, and then made available for further research.*
>
> [ ] *I consent*
>
> *You can withdraw your consent at any time by emailing researchconsent@researchproject.com.*

THIS IS VALID FOR GDPR CONSENT

- The consent concerns specifically the use of personal data
- All of the purposes for health data use are explicitly stated

- Date stamp and identity of person are captured, which creates a record of consent (alternatively, ask for a signature & date)
- The person is told about consent withdrawal and it is made easy

### 5.5.4. Sample consent – NOT VALID

*Web form for circulation at Company X, by area managers, to recruit volunteers for a wellbeing study.*

- *This research is described in the information sheet.*
- *Saliva samples will be collected.*
- *Participants are required to be available for two weeks for testing appointments.*

*As part of the background data collection, participants will be asked to fill in a short questionnaire:*

- *Job role, job duties, experienced stress levels, general health situation.*

*All data will be securely stored. By scrolling ahead, you are consenting to the above.*

THIS IS NOT VALID FOR GDPR CONSENT

- GDPR consent for personal data use is mixed with research participation consent
- It looks like the consent is asked at work, which *may* make GDPR consent invalid
- The personal data use purposes are not clearly stated (neither in the text or a linked notice)
- Health data is not recognised as special category data, requiring explicit consent
- The mechanism for giving consent is vague and does not leave a clear record
- No information is given about what is done with the data after the project
- No information of how to withdraw consent is given

# 6. Security guidelines/requirements

Mad@Work security guidelines are meant to provide IoT device related pilot programs with a set of security requirements that need to be followed in the pilot project implementation and deployment. The security guidelines are derived from industry best practices to holistically manage different aspects of information security in the pilot IoT solution delivery.

Current security guidelines are limited to IoT devices and associated services. The security guidelines may be further extended to cover also other IT systems and e.g. AI / ML based solutions.

## 6.1. Industry Best Practices

Following criteria frameworks are used when deriving Mad@Work security guidelines for IoT devices (excluding constrained devices):

| Criteria Framework | URL | Description | Applicability |
|---|---|---|---|
| NCSC-FI Cybersecurity Label | https://tietoturvamerkki.fi/en/requirements/ | Information security requirements targeted for IoT devices based on the ETSI EN 303 645 standard. | Consumer IoT devices and the associated services. |
| ETSI EN 303 645 V2.1.0 Cyber Security for Consumer Internet of Things: Baseline Requirements | https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf | The document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. | Consumer IoT devices and the associated services. |

The security guidelines are categorized under following high-level categories:

| Category | Description |
|---|---|
| Access Management | Controls related to protecting access to the consumer IoT devices and associated services. |

| Category | Description |
|---|---|
| Vulnerability Management | Controls related to insecure software components, vulnerability reporting, and software updates and patching. |
| Configuration, Key, and Secrets Management | Controls related to integrity and confidentiality of security configurations and secrets. |
| Communications Security | Controls related to securing data communications. |
| Hardening | Controls related to minimizing attack surface and hardening of the setup related to integrity controls. |
| Data Protection | Controls related to protection of personal and other sensitive data, including secure data deletion. |
| Business Continuity Controls | Controls related to resiliency in case of outages. |
| Detective Controls | Controls related to the ability to detect security events and anomalies. |

For each of the requirements, the following information is provided:

- Requirement identifier
- Requirement name
- Detailed description of the requirement
- Applicability
- Security objective
- References to the criteria framework
- Other additional information and references for additional materials

Current security requirements are put in place only for consumer IoT devices that are not constrained. The security requirements may be later extended to cover also backend services and other IT systems, and AI / ML functionalities.

## 6.2. Access Management

| PM-01 | Secure Password Management |
|---|---|
| Requirement | • When passwords are used, all IoT device passwords shall be unique per device or defined by the end-user.<br>• When pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks.<br>• Authentication mechanisms used to authenticate end-users against a device shall use best practice cryptography.<br>• Where an end-user can authenticate against a device, the device shall provide to the end-user or an administrator a simple mechanism to change the authentication value used.<br>• The device shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable. |
| Applicability | Consumer IoT devices |
| Security Objective | Consumer IoT devices are protected at an adequate level, so that unauthorised access to the device management is prevented. |
| References | NCSC-FI Cybersecurity Label requirement "2.1 Weak, Guessable, or Hardcoded Passwords"<br>ETSI EN 303 645 V2.1.0 requirement 5.1 "No universal default passwords" |

## 6.3. Vulnerability Management

| VM-01 | Process to Manage Reports of Vulnerabilities |
|---|---|
| Requirement | • Product manufacturer shall make a vulnerability disclosure policy publicly available.<br>• Disclosed vulnerabilities should be acted on in a timely manner. |

| VM-01 | Process to Manage Reports of Vulnerabilities |
|---|---|
| | • Product manufacturers should continually monitor for, identify, and rectify security vulnerabilities within their products and services. |
| Applicability | Consumer IoT devices |
| Security Objective | Keeping software vulnerability-related risks at a tolerable level. Ensuring transparency and clarity when interfacing with security researchers. |
| References | NCSC-FI Cybersecurity Label requirement "2.2 Use of Insecure or Outdated Components"<br>ETSI EN 303 645 V2.1.0 requirement 5.2 "Implement a means to manage reports of vulnerabilities" |
| **VM-02** | **Process to Keep Software Updated** |
| Requirement | • All software components in consumer IoT devices should be securely updateable.<br>• The device shall have an update mechanism for the secure installation of updates.<br>• An update shall be simple for the end-user to apply.<br>• Automatic mechanisms should be used for software updates.<br>• The device should check after initialization, and then periodically, whether security updates are available.<br>• If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the end-user can enable, disable, or postpone installation of security updates and/or update notifications.<br>• The device shall use best practice cryptography to facilitate secure update mechanisms.<br>• Security updates shall be timely.<br>• The device should verify the authenticity and integrity of software updates.<br>• Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.<br>• The manufacturer should inform the end-user in a recognizable and apparent manner that a security update |

| VM-01 | Process to Manage Reports of Vulnerabilities |
|---|---|
| | is required together with information on the risks mitigated by that update.<br>• The device should notify the end-user when the application of a software update will disrupt the basic functioning of the device. |
| Applicability | Consumer IoT devices |
| Security Objective | Keeping software vulnerability-related risks at a tolerable level. |
| References | NCSC-FI Cybersecurity Label requirement "2.2 Use of Insecure or Outdated Components"<br>ETSI EN 303 645 V2.1.0 requirement 5.3 "Keep software updated" |

## 6.4. Configuration, Key, and Secrets Management

| CMKS-01 | Process to Securely Store Sensitive Configuration Parameters |
|---|---|
| Requirement | • Sensitive security parameters in persistent storage shall be stored securely by the device.<br>• Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.<br>• Hard-coded critical security parameters in device software source code shall not be used.<br>• Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.<br>• The manufacturer shall follow secure management processes for critical security parameters that relate to the device. |
| Applicability | Consumer IoT devices |

| CMKS-01 | Process to Securely Store Sensitive Configuration Parameters |
|---|---|
| Security Objective | Protecting sensitive information in configuration parameters from unauthorized access. |
| References | NCSC-FI Cybersecurity Label requirement "2.4 Insecure Data Transfer and Storage"<br>ETSI EN 303 645 V2.1.0 requirement 5.4 "Securely store sensitive security parameters"<br>ETSI EN 303 645 V2.1.0 requirement 5.5 "Communicate securely" |

## 6.5. Communications Security

| CS-01 | Process to Ensure Secure Communications |
|---|---|
| Requirement | • The consumer IoT device shall use best practice cryptography to communicate securely.<br>• The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.<br>• Cryptographic algorithms and primitives should be updateable.<br>• Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.<br>• Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication.<br>• Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.<br>• The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces. |
| Applicability | Consumer IoT devices |

| CS-01 | Process to Ensure Secure Communications |
|---|---|
| Security Objective | The confidentiality or integrity of end-user personal data is not compromised in transfer through unreliable networks. |
| References | NCSC-FI Cybersecurity Label requirement "2.4 Insecure Data Transfer and Storage"<br>NCSC-FI Cybersecurity Label requirement "2.5 Insecure Network Services and Ecosystem Interfaces"<br>ETSI EN 303 645 V2.1.0 requirement 5.5 "Communicate securely" |

## 6.6. Hardening

| HD-01 | Minimize Attack Surface |
|---|---|
| Requirement | • All unused network and logical interfaces shall be disabled.<br>• In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.<br>• The manufacturer should only enable software services that are used or required for the intended use or operation of the device.<br>• Code should be minimized to the functionality necessary for the service/device to operate.<br>• Software should run with least necessary privileges, taking account of both security and functionality.<br>• The device should include a hardware-level access control mechanism for memory.<br>• The manufacturer should follow secure development processes for software deployed on the device. |
| Applicability | Consumer IoT devices |
| Security Objective | Reduces the risk of software flaws and faulty configurations by removing from use functionalities that are not needed. |
| References | NCSC-FI Cybersecurity Label requirement "2.5 Insecure Network Services and Ecosystem Interfaces" |

| HD-01 | Minimize Attack Surface |
|---|---|
| | ETSI EN 303 645 V2.1.0 requirement 5.6 "Minimize exposed attack surfaces" |
| **HD-02** | **Process to Ensure Software Integrity** |
| Requirement | • The consumer IoT device should verify its software using secure boot mechanisms. |
| Applicability | Consumer IoT devices |
| Security Objective | The integrity, confidentiality, or availability of end-user personal data are protected at an adequate level against common malware risks. |
| References | ETSI EN 303 645 V2.1.0 requirement 5.7 "Ensure software integrity" |

## 6.7. Data Protection

| DP-01 | Process to ensure that personal data is secure |
|---|---|
| Requirement | • The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.<br>• The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.<br>• All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the end-user. |
| Applicability | Consumer IoT devices |
| Security Objective | End-user's personal data to be kept secret can only be accessed by the end-user in question. |

| DP-01 | Process to ensure that personal data is secure |
|---|---|
| References | ETSI EN 303 645 V2.1.0 requirement 5.8 "Ensure that personal data is secure" |
| **DP-02** | **Process to delete end-user personal data** |
| Requirement | • The end-user shall be provided with functionality such that end-user data can be erased from the device in a simple manner.<br>• The end-user should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.<br>• End-users should be given clear instructions on how to delete their personal data.<br>• End-users should be provided with clear confirmation that personal data has been deleted from services, devices and applications. |
| Applicability | Consumer IoT devices |
| Security Objective | The confidentiality of a end-user's personal data to be kept secret is not compromised when device or associated services used for the processing of the information are taken out of use or the end-user's personal data must be deleted from the device and associated services for other reasons. |
| References | ETSI EN 303 645 V2.1.0 requirement 5.11 "Make it easy for users to delete user data" |

## 6.8. Business Continuity Controls

| BC-01 | Process to ensure resiliency against outages |
|---|---|
| Requirement | • Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power<br>• Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power. |

| BC-01 | Process to ensure resiliency against outages |
|---|---|
| | • The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration. |
| Applicability | Consumer IoT devices |
| Security Objective | The objective of continuity management is to ensure the continuity of service so that it is possible to meet the availability, integrity and confidentiality requirements associated with the service. |
| References | ETSI EN 303 645 V2.1.0 requirement 5.9 "Make systems resilient to outages" |

## 6.9. Detective Controls

| DC-01 | Process to examine telemetry data |
|---|---|
| Requirement | • If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies. |
| Applicability | Consumer IoT devices |
| Security Objective | Detection of any unauthorised alteration to information or other unauthorised or inappropriate information processing, including detection of security breaches and support for the planning of corrective measures. |
| References | ETSI EN 303 645 V2.1.0 requirement 5.10 "Examine system telemetry data" |

# 7. Ethics guidelines/requirements

## 7.1. Informed Consent

Note: It is important to note that informed consent for research participation and GDPR consent for personal data processing are two distinct consents that can exist at the same time.

### *7.1.1.* Informed consent in research

The foundations of informed consent principles are based in on the Declaration of Helsinki and on similar documents including EU's informed consent principles in the Europe.

Informed consent is defined a subject's free and voluntary expression of his or her willingness to participate in a particular study, after having been informed of all aspects of the study that are relevant to the subject's decision to participate or, in case of minors and of incapacitated subjects, an authorization or agreement from their legally designated representative to include them in the study.

Informed consent obligations that Mad@Work research pilots follow:

- Informed consent must be dated and signed by the person providing the information and the subject must be given a copy of the document. Adequate time must be given to the person to ask questions and understand the information presented.
- The informed consent process must permit the subject to understand:
- The nature, objectives, expected benefits, implications, risks and inconveniences of the study.
- The subject's rights and guarantees regarding his or her protection, in particular his or her right to refuse to participate and the right to withdraw from at any time without having to provide any justification.
- The conditions under which the study is to be conducted, including the expected duration of the subject's participation.
- The information given to the subject must be complete, easy to understand, concise and relevant.
- The information must be given by a qualified individual prior to any research activities.
- Damage compensation must be discussed.
- Availability of study results must be described.

# 8. Conclusions

This deliverable *D2.1 - User and technical requirements, pilot specifications* produces a much more detailed overview of the different pilots which will be deployed in Mad@Work, as well as a first understanding of commonalities and differences between them. Additionally, it also provides a global overview about how the Mad@Work solution can be deployed in real-life settings.

At this point, it is already possible to differentiate three kinds of pilots:

**Pilots focused on the knowledge workers**, like Pilot 1 - Stress detection and mitigation in location-independent people working in front of a PC (led by Hi-Iberia), Pilot 3 – Stress and performance in location independent office workers (led by FIOH & VTT) and Pilot 6 - Early Detection of Stress in the Workplace

**Pilots focused on the workplace environment**, like Pilot 2 – Personalized Lighting in Indoor Work Spaces (led by Helvar), Pilot 4 - Learning facility (led by Granlund) and Pilot 5 - Safe to breath (led by UniqAir)

**Hybrid pilot** like Pilot 7 - Pilot WellMind (led by ETRI)

All of them will follow the overall vision of the Mad@Work solutions, which is explained in the deliverable D2.2.

This deliverable builds the project basis and it can be considered as an essential piece of work in the Mad@Work definition phase. In fact, a first understanding of the target scenarios (pilots) is essential to start outlining some of the more technical aspects. In this way, it is shown in the below figure:

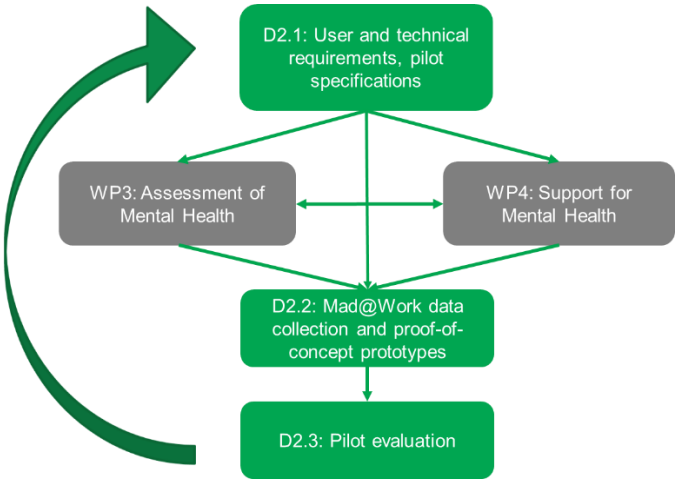



*Figure 10 - Positioning D2.1 in the project*

As it can be seen, this work will finally evolve into fully featured pilots which allow to be validated against user requirements and the benefits evaluated to check progress against project KPIs.

.

# 9. Appendix 1 – Mad@Work cross-cultural questionnaire

---

This survey is a part of international research project Mad@Work under ITEA 3 programme. The goal of Mad@Work project is to develop stress assessment and intervention applications and this way to improve wellbeing at work. By answering these questions, you would help us to develop these applications.

The survey takes about XX minutes, and it is completely anonymous. Data will be used for research purposes only.

The survey is open until xx.xx.2021.

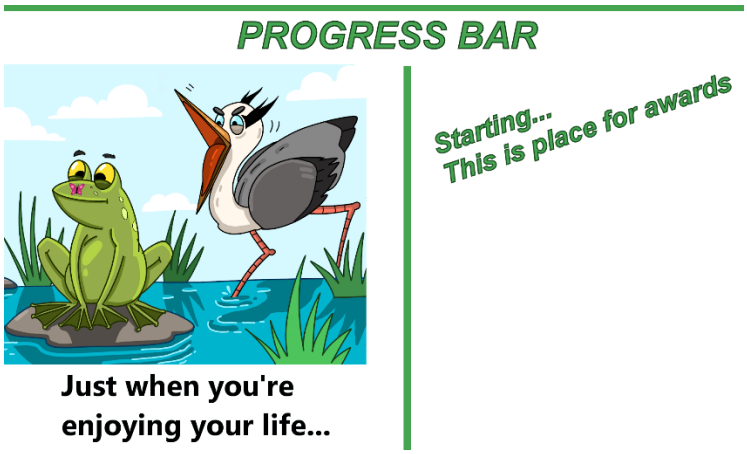
Progress of answering this survey is displayed via standard progress bar and additionally via pictorial progress bar. Images in the pictorial progress bar do not reflect contents of the questions.

Thank you very much in advance, your opinion is highly appreciated!

***Background***

1. Age
    a. < 25
    b. 25-35
    c. 35-45
    d. 45-55
    e. > 55
2. Gender
3. Education
    a. primary education
    b. secondary education
    c. Bachelor's level
    d. Mater's level
    e. Doctoral
4. Nationality
5. Workplace:
    a. Public sector
    b. Private sector
    c. Other (e.g. a non-profit company /organization)
6. Position
    a) Manager
    b) Professional
    c) Technicians and associate professional
    d) Service, sales or clerical support worker
    e) Other

7. Your English language proficiency. Please check the option that applies.
    a. Basic user
    b. Intermediate user
    c. Proficient user
    d. Native speaker



8. Do you have experience in using stress detection and intervention apps, smart watches etc.,?
   Likert scale: None - very much

9. Stress means a situation in which a person feels tense, restless, nervous or anxious or is unable to sleep at night because his/her mind is troubled all the time. Do you feel this kind of stress these days?
   - Not at all
   - Very little
   - Somewhat
   - Quite Much
   - Very Much

10. How worried are you about your stress?
    - Not at all
    - Very little
    - Somewhat
    - Quite Much
    - Very Much

11. Do you consider those as noise?
    - conversations in the background/corridor
    - headphone music
    - construction sound
    - lamps, fridge, etc..

12. How important are to you the following aspects your work environment
    - ecologic materials
    - saving energy
    - aesthetics (chair, table, light)
    - greenness, plants
    - organised / not messy work space

13. If you need to choose, which work aspects would you value higher?

    - work challenges vs. work predictability, no or little overwork.

    Likert: 1/work challenges, 2/rather work challenges 3/both are equally important, 4/rather work predictability, 5/work predictability

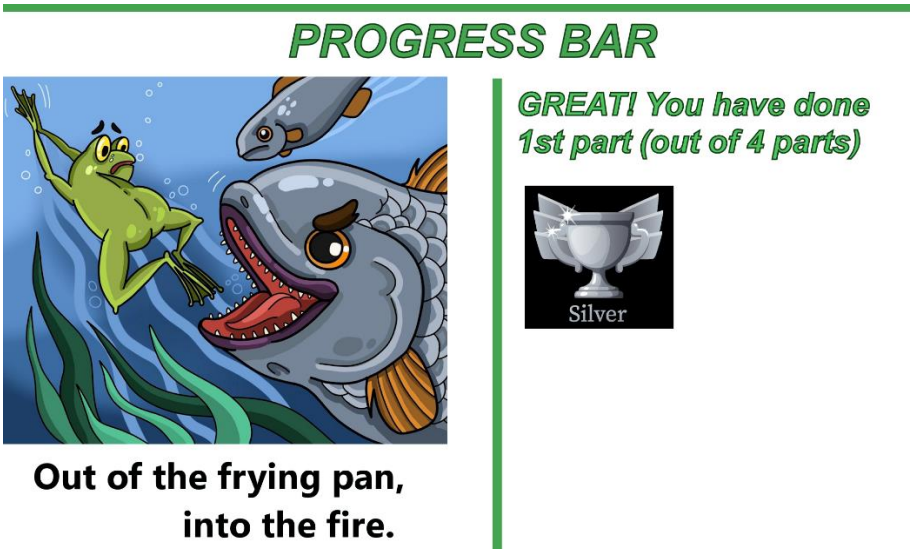
    - good relations with colleagues vs. efficient work outcome

    Likert: 1/good relations with colleagues, 2/rather good relations with colleagues, 3/both are equally important, 4/rather efficient work outcome, 5/efficient work outcome

14. What are the top aspects of yourself that you would be interested in measuring automatically throughout your day and night?
    (check box: “select all that applies”)

    - How well I sleep
    - My stress levels
    - My mood or emotional states
    - My Concentration/attention
    - Use of my work and leisure time
    - Calories burned
    - How far I walk, run or cycle
    - Whether I am dehydrated
    - My weight
    - My blood pressure
    - My heart rate
    - How long I spend sitting
    - My Cognitive load /resources
    - My recovery status
    - Other:
    - None

Optional: Please explain your answer for the above question. Why would you be interested in these aspects?



15. What are your top motivations to track yourself?
(check-boxes: “select all that applies”)

- To achieve some goal
- To be mindful and to find balance
- To document my life accurately
- To understand myself better
- To understand how this factor relates to others (for example, the impact of focus on mood)
- To explore a new technology
- To satisfy curiosity and to have fun
- To predict how I will do in the future
- To increase my health and well-being
- Other:
- Don’t know/unsure
- None

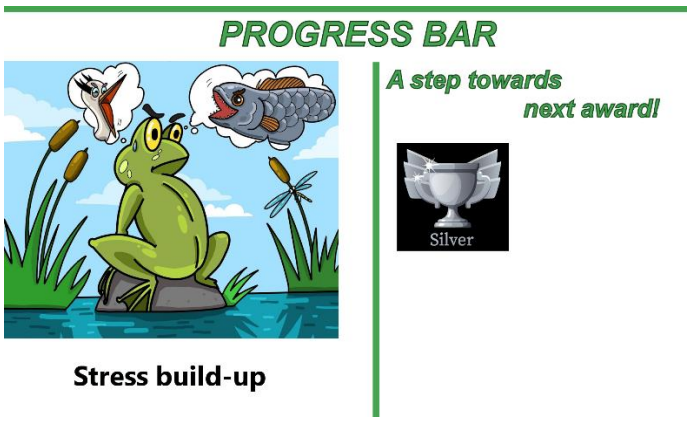
Optional: Please explain your answer for the above question. Why are these your top motivations?

16. What are your top inhibiting factors to track yourself? (check-boxes: “select all that applies)

- Wellbeing applications cost too much
- I do not want to be dependent on the wellbeing applications
- Using wellbeing applications takes too much of my time
- Using and understanding wellbeing applications is difficult
- I am concerned about the use of collected data
- I am generally sceptical to technology
- None

17. At my workplace, I talk about my private life and issues with the colleagues

- never
- rarely
- sometimes
- often
- all the time / always
- anything else, free text



***Beliefs and expectations***

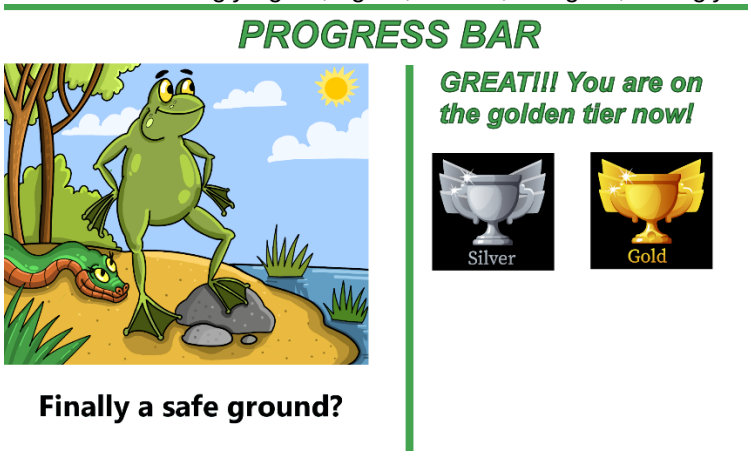
18. Imagine that stress detection application says that you are stressed, but you have not noticed it yourself. What would you do: (one choice radio button?)
    - I would believe the stress assessment application because it is specially designed to assess stress
    - I would do nothing now, but would pay special attention to my mental state during next month and this way would test the stress assessment application
    - I would stop using the stress assessment application because it made a mistake
    - anything else? free text

19. What do you think, how good are currently available stress assessment applications?
    - they almost never make mistakes, like in 0-5% of cases
    - they make mistakes seldom, like in 5-15% of cases
    - they make mistakes sometimes, like in 15-25% of cases
    - they make mistakes often, like in 25-40% of cases
    - they make mistakes almost always: in more than 40% of cases
    - anything else, free text

20. Would you be interested in the reasons for wrong stress detection results? One example: “the application cannot detect stress during the days when the user is not using his/ her computer or phone”. Another example: “the application may decide that the user is stressed if the user was walking fast even if the user is happy”.
    - Very interested
    - Interested
    - Difficult to say / moderately
    - Not so interested
    - Not at all interested
    - Anything else? Free text

21. If stress detection applications are used in your workplace, do you agree that they will ensure the security of your personal data?
    - Strongly agree, agree, neutral, disagree, strongly disagree

22. Do you agree that stress detection applications are created for the good of human being?
    - Strongly agree, agree, neutral, disagree, strongly disagree



***Personal stress management***

23. Do you think a stress assessment and management app would be useful for you? (This app would detect your stress and advise you how to relieve it) Likert Scale:
    - Very useful
    - Somewhat useful
    - Indifferent
    - Not useful
    - Can be harmful

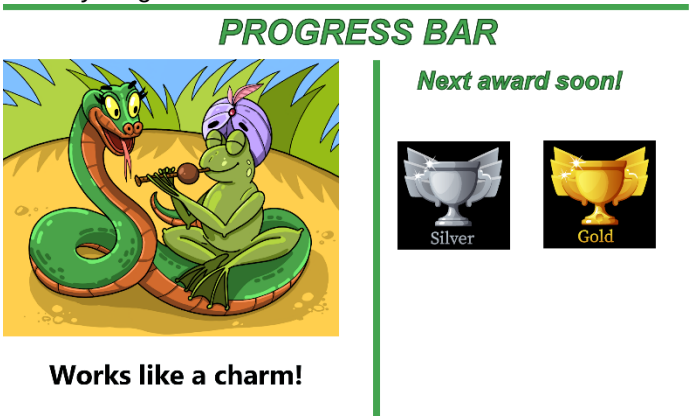
24. Would you be interested in learning stress management skills, provided by an application, that can improve your general ability to cope with stressful situations? (5-point Likert scale; not at all - Extremely)

    19.a If yes, how much time per week would you be ready to spend to learn these skills?

    - ½h
    - 1h
    - 2h
    - 3h or more

25. Which of the following stress relief methods you have used or would like to use? (Check boxes: select all that applies)
    - walking
    - exercising
    - watching video/VR (e.g. nature viewing)
    - stretching
    - meditation
    - yoga
    - relaxation
    - biofeedback
    - napping
    - sleep enhancement
    - proper work brakes
    - socialising with colleagues
    - balanced diet
    - listening to music or nature sounds
    - aromatherapy
    - None of above
    - Other:

26. Imagine that you have an individual support tool helping you to monitor your stress level. Which way would you prefer to interact with this tool?
    - to receive notifications when your stress level is too much worrying
    - to receive notifications when your stress level is increasing with regards to the previous hours.
    - no notifications about your stress level: you access this information when you consider necessary.
    - anything else?

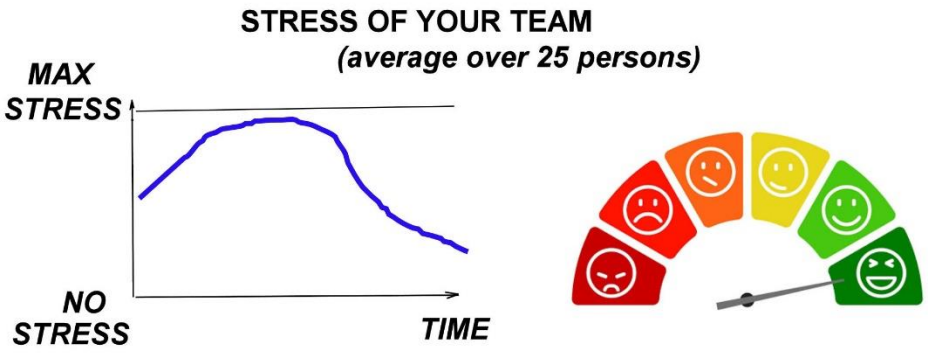


***Organisational stress management***

27. Would you be interested in the following information about your organization/research team? (Check boxes: “select all that applies”)
    - General stress level or emotional state of your team/ organizational unit
    - Workload level/ how busy colleagues are
    - Workplace satisfaction level
    - Motivation level
    - Workplace social comfort level
    - Level of trust in the leadership
    - Self-reliance (autonomy) level
    - What are your colleagues busy with: topics, projects, activities
    - Interests, hobbies of your colleagues
    - None of above
    - Other:

28. What kind of accuracy versus frequency of results compromise (trade-off) would you prefer:
    - more frequent, but less accurate reporting
    - less frequent, but more accurate reporting
    - something else? free text

29. Would you be interested in **anonymously aggregated collective stress level of your team**/ organisational unit? Examples of displaying the average collective stress levels are in the pictures below.

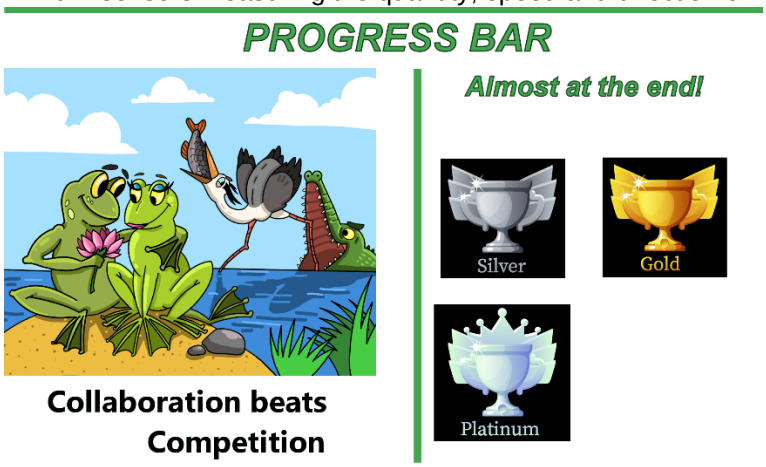



(one choice radio button?)

- I would provide my stress data to be aggregated, without any conditions
- I would not provide my stress data for this purpose
- I would provide my stress data to be aggregated, but with the following conditions: (multiple choice check box)
    - if I was able to control when and what data are collected
    - if I was able to completely trust that my data are only used for a certain fair purpose
    - if I was able to completely trust that it did not result in any actions that would affect me or my team negatively
    - if I also received direct benefits for myself
    - Other, free text?

***Stress data collection***

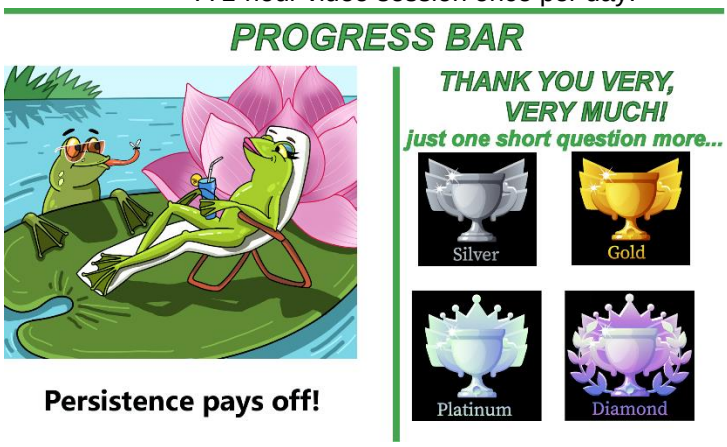
30. Your stress and work environment can be monitored using various sensors, and the more sensors are used, the more accurate results can be expected. Continuous monitoring is expected to provide more accurate results than periodic data collection. Then, what kind of data would you allow to collect and how? Likert Scale: 1-5: Strongly agree, agree, neutral, disagree, strongly disagree.
    - I would allow collecting physiological data (e.g. heart rate, respiratory rate, blood pressure, temperature)
        a. Using smart watch to record data continuously during working hours
        b. Using fingertip biosensor to record data periodically during working hours
    - I would allow collecting video data (facial expression, movements, eye gaze, heart rate)
        a. Using a video camera installed in the office room to record data continuously during working hours
        b. Using my PC webcam to record several short video-sessions during working hours
        c. Using my smartphone camera to record several short video-sessions during working hours
    - I would allow collecting motion data using sensors, installed in the office, continuously during working hours. (Motion sensors cannot identify persons).
        a. sensors measuring only the motion quantity
        b. sensors measuring the quantity, speed and direction of motion



- I would allow collecting data about my use of the following devices continuously during working hours. Data about the content (e.g., used programs, websites, written text/keystrokes, voice etc.) are not collected
    a. computer usage data (program categories, duration, typing/clicking tempo)
    b. mobile phone usage data (program categories, duration, typing/clicking tempo)
- I would allow collecting environmental quality data from my work space using the following sensors continuously during working hours.
    a. Sound level
    b. Air quality
    c. Temperature
    d. Lighting
    e. Humidity
- I would periodically report my feelings explicitly, using
    a. detailed self-reporting form/application
    b. smiling face or thumb
    c. interactive discussion forum
    d. other

30.a, for subjects who answered “I would allow collecting video data”:
Let’s suppose the stress detection is carried out with short video sessions. How long would you rather be being recorded by your computer webcam or mobile camera during the working hours? Likert Scale: 1-5.

- A 3-minutes video session for each hour.
- A 5-minutes video session five times per day
- A 10-minutes video session three times per day
- A 30-minutes video session twice per day
- A 1-hour video session once per day.




---

***Gamification***

We need to track who started and who finished, and if the user stopped, at which question it happened. We will randomly assign subjects to 2 gamification stories and “no gamification” option. If a subject gets gamification, we will ask:

For subjects with gamification: (5-point Likert)

31. What do you think, were the pictures of the progressing story a good addition for you, or were they annoying?
    - I disliked the progressing story very much
    - I disliked the progressing story
    - I am indifferent
    - I liked the progressing story
    - I liked the progressing story very much

# 10. Appendix 2: Preliminary results from Mad@Work cross-cultural questionnaire

The questionnaire has already been launched. To date, it was answered by 443 respondents: 218 female, 219 male, and 6 opted not to disclose. Here we present only preliminary results and only a summary of responses to general questions about overall Mad@Work approach because we plan to publish full analysis of the results in a paper, after we collect more responses.

Age and education distribution of the respondents are presented in the tables below.

| Age | Number of persons | Percentage |
|---|---|---|
| **<20** | 3 | 0,7 |
| **20-29** | 88 | 19,9 |
| **30-39** | 106 | 23,9 |
| **40-49** | 115 | 26,0 |
| **50-59** | 95 | 21,4 |
| **>60** | 36 | 8,1 |
| **Total** | 443 | 100,0 |

*Table 1- Age distribution of the respondents*

| Education | Number of persons | Percent |
|---|---|---|
| **Primary education** | 3 | ,7 |
| **Secondary education** | 17 | 3,8 |
| **Bachelor's level** | 71 | 16,0 |
| **Master's level** | 185 | 41,8 |
| **Doctoral** | 167 | 37,7 |
| **Total** | 443 | 100,0 |

*Table 2 - Education of the respondents*

General questions regarding planned applications are Q_23 (individual support) and Q_29 (organizational barometer).

Regarding Q_23, individual support, 52.2% (the majority of the respondents) expressed positive attitude (“somewhat needed” or “very necessary”), 19.8% expressed negative attitude (“not needed” or “can be harmful”), and 28% were neutral.

Regarding Q_29, only 5.2% of the respondents answered “I would not allow my organisation to use my stress data for this purpose”, whereas 34.1% answered “I would allow my stress data to be aggregated without any conditions”. Others answered that they would allow data aggregation conditionally, the top two conditions being “if I was able to completely trust that my data are only used for a certain fair purpose” and “if I was able to completely trust that it did not result in any actions that would affect me or my team negatively”.

We consider these results encouraging because to the question “How worried are you about your stress?” 31.6% of the respondents answered that they worry very little or not at all. Thus it seems that even if an individual is not worried about his/ her stress, he/ she would nevertheless interested in individual and/ or organisational support tools. More detailed correlations between the interest in support tools and personal background will be done later.

Regarding sensor-based monitoring and explicit reporting (Q30), the majority of respondents would allow collection of at least one type of sensor data, and over 40% of the respondents would periodically express their feelings explicitly.

Regarding choice of sensor data types, physiological sensors were the most popular, but it may be partially because wearables are widespread and not perceived as “Big Brother” tools, whereas video and computer usage data collection tools are traditionally perceived as such. We plan to compare attitudes to different sensors prior to pilots with the attitudes after the pilots and with the personal background, especially his/ her experience in using wearables and sensor management applications (background question Q8). In any case, preferences for different sensors varied between the subjects, which means that Mad@Work approach to not focus on a single sensor is feasible.

One interesting result is that the respondents did not perceive available stress assessment applications as highly accurate (Q19): only 14% of the respondents evaluated them as making mistakes in less than 15% of cases, whereas about 1/3 answered “I do not know”. This result suggests that knowledge workers do not have unrealistic accuracy expectations and hence real-life stress detectors, which cannot achieve high accuracies, may nevertheless be well accepted.

# 11. Appendix 3: Data protection by design guidelines

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| GDPR Principle: Transparency | | | | |
| 1 | Clarity | Information shall be in clear and plain language, concise and intelligible. | "Information" refers to information about how the individual's data is processed in the solution. The solution provider should provide it to the employer (data controller) who should use it to inform its employees (data subjects). The information may be provided for example as part of the solution description or in a **partially filled privacy notice template.** | "Information" refers to information about how the individual's data is processed in the solution. The solution provider should provide it directly to the individual - usually in the form of a privacy notice.<br>In addition to a privacy notice, the information should be provided in a "user friendly" way: illustrations, user guides, animation, FAQs etc. |
| 2 | Semantics | Communication should have a clear meaning to the audience in question. | The first hand audience is the employer, but the end audience is the employees. When communicating to the employer, it is a good idea to use terminology that also the employees would understand. | The technical solution may be difficult to understand or difficult terms may be in use, which should be explained so that the individual understands them. Illustrations or animation could be used. |
| 3 | Accessibility | Information shall be easily accessible for the data subject. | Ensure that the end user interface has a place for a link to the employer privacy notice. Also, consider all the different ways that you as the solution provider can make access to privacy information easier - for example through a built-in "privacy dashboard".<br>Also regard the EU Web Accessibility Directive. | Ensure that the end user interface has a link to your company privacy notice.<br>In addition, informative material should also be easily available through the user interface - for example through a built-in "privacy dashboard".<br>Also regard the EU Web Accessibility Directive. |
| 4 | Contextual | Information should be provided at the relevant time and in the appropriate form. | Consider when the end user accesses the solution for the first time or provides data through the solution.<br>For example, can features be added that would explain the user why the data is needed, e.g. small info pop-ups or help text. Perhaps, a video that explains how their data is used is appropriate, if the | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | processing is complex and is better explained.<br><br>Also, visual indicators can be used to show that data collection is in progress, such as a red 'recording' light. | |
| 5 | Relevance | Information should be relevant and applicable to the specific data subject. | When designing transparency features for the solution, try to anticipate what the end users (employees) might worry about regarding their data and privacy. Try to address their concerns. | ← as Scenario 1 |
| 6 | Universal design | Information shall be accessible to all data subjects, include use of machine readable languages to facilitate and automate readability and clarity. | The solution provider should consider accessibility of the privacy features. | ← as Scenario 1 |
| 7 | Comprehensible | Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups. | This aspect should be included in the user experience design. The solution provider could test this aspect with users. | ← as Scenario 1 |
| 8 | Multi-channel | Information should be provided in different channels and media, not only the textual, to increase the probability for the information to effectively reach the data subject. | As the solution provider, consider imaginative ways of making the employee's data use more transparent to them. For example, when the solution is recording/collecting data, a red light is shown. Or, the employee is given a chance to review the data before sending it to further processing. | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| 9 | Layered | The information should be layered in a manner that resolves the tension between completeness and understanding, while accounting for data subjects' reasonable expectations. | The employer (data controller) usually writes a privacy notice that includes the necessary information. As the solution provider, please ensure that there is a place where the privacy notice or a link to a privacy notice may be inserted.<br><br>However, privacy notices tend not to be very user-friendly. As the solution provider, provide end-users information about how the system works and uses personal data in a "user friendly" way: illustrations, user guides, animation, FAQs etc. Consider the employee user journey and what information about their data use and privacy they might wish to receive at each stage. Aim to build it in the solution. | Privacy notices tend not to be very user-friendly. It can be available on the background. In addition to a privacy notice, provide information in a "user friendly" way: illustrations, user guides, animation, FAQs etc. Consider the employee user journey and what information about their data use and privacy they might wish to receive at each stage. Aim to build it in the solution. |
| GDPR Principle: Lawfulness | | | | |
| 10 | Relevance | The correct legal basis shall be applied to the processing. | The solution provider should anticipate what GDPR legal basis/bases the employer will have at its disposal for the solution. Especially the following should be considered:<br><br>• Use of consent as a legal basis in employment context may not be possible<br>• There may be local employment privacy laws that may prevent the solution to be used or add limitations or special requirements. (See GDPR Article 88 and Recital 155) | The solution provider should define what GDPR legal basis it will use for each purpose it has for the personal data. Especially the following should be considered:<br><br>For the processing of ordinary personal data<br><br>• Contract<br>• Consent<br>• Legitimate interest<br>For the processing of special category data (such as health data)<br><br>• Explicit consent |
| 11 | Differentiation | The controller shall differentiate between the legal basis used for each processing activity. | The solution provider should anticipate how the solution's functions guide what GDPR legal basis/bases may apply to them. Different functionalities may be | As above. |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | communicated to the employer in logical groupings, such as:<br>• functionality relating to an employer's legal duties<br>• functionality relating to voluntary information (consent?) | |
| 12 | Specified purpose | The appropriate legal basis must be clearly connected to the specific purpose of processing. | Consider a scenario where the employer cannot take all functionalities into use, because it cannot find a legal basis for processing data in that context, and offer a way to switch off these functionalities. | Be ready to justify how they connect. |
| 13 | Necessary | Processing must be necessary for the purpose to be lawful. It is an objective test which involves an objective assessment of realistic alternatives of achieving the purpose. | Consider grouping the functionalities of the solution in terms of necessity. This can help the employer to choose those that it can justify as being necessary for the employer's purpose/use case.<br><br>(It is the employer's responsbility to assess whether it is necessary to process the employees' data that way.)<br><br>Legitimate interest: If you want to use the data for your own purposes such as security, marketing or solution development, you must be able to justify that it is necessary (to the extent you are doing it). | Contract: Consider the service that you are offering to the end users, and design the solution so that it processes their data only to the extent necessary for providing the advertised service.<br><br>Legitimate interest: If you want to use the data for your own purposes such as security, marketing or solution development, you must be able to justify that it is necessary (to the extent you are doing it). |
| 14 | Autonomy | The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data. | Consider including a privacy dashboard for the employees. Consider including functionality for employees to:<br>• turn data collection methods on/off, perhaps method by method<br>• control who can use/see their data<br>• control what purposes their data may be used | ← as Scenario 1, for end users |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | • access their data to see what has been collected<br>• correct their data<br>• pause the processing<br>• etc.<br>Remember to make the default setting the most privacy-preserving. | |
| 15 | Consent withdrawal | The processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid. | If the solution includes any voluntary options or consents for the end user, ensure that they can change them whenever and easily. | ← as Scenario 1 |
| 16 | Balancing of interests | Where legitimate interests is the legal basis, the controller must carry out an objectively weighted balancing of interests. There shall be measures and safeguards to mitigate the negative impact on the data subjects, and the controller should disclose their assessment of the balancing of interests. | Legitimate interest: If you want to use the data for your own purposes such as marketing or solution development, you must be able to justify that it is necessary (to the extent you are doing it) - you can document this in a LIA (Legitimate Interest Assessment). | ← as Scenario 1 |
| 17 | Predetermination | The legal basis shall be established before the processing takes place. | (nothing to add) | ← as Scenario 1 |
| 18 | Cessation | If the legal basis ceases to apply, the processing shall cease accordingly. | Consider adding technical ways of stopping processing when it is needed, and note that processing includes storage as well. | Contract: The solution should be designed so that when the contract with the end user ends, all processing (incl. data storage) also ends. (Note: At that point, you may have a |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | | legitimate interest to keep some of the data for your own purposes.)<br><br>Consent: When consent is withdrawn, the solution should stop processing that data. |
| 19 | Adjust | If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis. | (nothing to add) | An example of this may be that the contract with end user ends, but you wish to retain some of the data for your own purposes. You need to consider what data you might be able to justify to kept. |
| 20 | Default configurations | Processing must be limited to what the legal basis strictly gives grounds for. | (nothing to add) | ← as Scenario 1 |
| 21 | Allocation of responsibility | Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject | (nothing to add) | ← as Scenario 1 |
| GDPR Principle: Fairness | | | | |
| 22 | Autonomy | Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing. | See 14 (privacy dashboard). | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| 23 | Interaction | Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller. | See 14 (privacy dashboard).<br><br>See 1. The template should have space for controller details and information about exercising one's rights (with details how they can be exercises through the privacy dashboard if one is in place). | See 14.<br><br>See 1. The notice should include details of the controller and information about exercising one's rights (with details how they can be exercises through the privacy dashboard if one is in place). |
| 24 | Expectation | Processing should correspond with data subjects' reasonable expectations. | Consider doing research with end users to find out about their expectations about the use of their data in the kind of a solution you are designing for.<br><br>Review related literature. | ← as Scenario 1 |
| 25 | Non-discrimination | The controller shall not unfairly discriminate against data subjects. | Consider whether the design of the solution can expose employees to discrimination. Consider whether the employer could (mis)use your solution in a discriminatory way. Try to mitigate these.<br><br>Especially consider whether any of the following characteristics of employees relate to the solution: sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, disability, age or sexual orientation.<br><br>Examples:<br><br>• employee suffers unfair disadvantage - does not get the same benefits, cannot use the solution like others, gets inappropriate and badly judged recommendations etc,<br>  ○ a woman's hormonal changes, person's religious practices or physiological | ← as Scenario 1, but consider end users. |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | ○ illness affect their data or behaviour or options available for them<br>○ system does not detect mood from a black person's face<br>○ sensor does not detect a disbaled person's form as a human form<br>○ etc. | |
| 26 | Non-exploitation | The controller should not exploit the needs or vulnerabilities of data subjects. | Consider, does the solution trade something between the employer and employees, and whether this is fair for the employees - are they pushed for example to give out more data for some benefit that they would normally get anyway? Note that GDPR recognises employees as vulnerable data subjects in relation to their employer.<br><br>Consider how the solution treats highly stressed persons. Could it lead to their exploitation e.g. for collecting extra data for product development from stressed persons.<br><br>Consider whether including gamified features with highly stressed persons could lead to their exploitation, e.g. getting them hooked on the solution. | Consider how the solution treats highly stressed persons. Could it lead to their exploitation e.g. for collecting extra data for product development from stressed persons.<br><br>Consider whether including gamified features with highly stressed persons could lead to their exploitation, e.g. getting them hooked on the solution. |
| 27 | Consumer choice | The controller should not “lock in” their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a | Build an easy data export functionality for the employees. See 14.<br><br>Where possible, aim for data formats that can be transferred to other similar solutions, for if not all, then for part of the data. | ← as Scenario 1, for end users. |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | lock-in to the service, which may not be fair, if it impairs the data subjects' possibility to exercise their right of data portability in accordance with Article 20. | | |
| 28 | Power balance | Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures. | Power imbalance exists in the employee-employer relationship. See 14 for potentail mitigations. | Consider highly stressed end users. See 14 for potential mitigations. |
| 29 | No risk transfer | Controllers should not transfer the risks of the enterprise to the data subjects. | (This is the employer responsibility. For example, transferring employee wellbeing management to employees themselves to manage through the solution is questionable.) | - |
| 30 | No deception | Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design. | Ensure that the GUI design does not manipulate users to provide data and that all voluntary options are clearly come across as such.<br><br>Remember cookie consent notices (see recent complaints). | ← as Scenario 1 |
| 31 | Respect rights | The controller must respect the fundamental rights of data subjects and implement | Consider the fundamental rights of dignity, freedoms, equality, solidarity, citizens' rights and justice (simple summary) and | ← as Scenario 1, for end users. |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | appropriate measures and safeguards and not impinge on those rights unless expressly justified by law. | whther they can be affected in this solution. | |
| 32 | Ethical | The controller should see the processing's wider impact on individuals' rights and dignity. | To help the employer to understand wider issues, the solution provider could carry out a modelling exercise of the wider impact and illustrate the results in the solution documentation. A systemic modelling method can work well to gain a wider view. | A systemic modelling method can work well to gain a wider view. The results should then be used to improve the solution. |
| 33 | Truthful | The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects. | See 1, 2, 5 and 7. | ← as Scenario 1 |
| 34 | Human intervention | The controller must incorporate qualified human intervention that is capable of uncovering biases that machines may create in accordance with the right to not be subject to automated individual decision making in Article 22. | Consider how humans can oversee and intervene in the use of artificial intelligence in the solution and is this done by you as the solution provider or the employer or both. | ← as Scenario 1 (but employer does not need to be considered). |
| 35 | Fair algorithms | Regularly assess whether algorithms are functioning in line with the purposes and adjust the | Document the schedule and procedures for assessments as well as the completed assessments. They will acts as an important proof of compliance. | ← as Scenario 1, but inform data subjects directly, for example on your website. |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | algorithms to mitigate uncovered biases and ensure fairness in the processing. Data subjects should be informed about the functioning of the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements. | Taking guidance from the Transparency section, produce easy to understand information that the employer can use in informing their employees (or provide it on your webiste for the employees to refer to directly). | |
| GDPR Principle: Purpose limitation | | | | |
| 36 | Predetermination | The legitimate purposes shall be determined before the design of the processing. | Legitimate interest of the solution provider: If you want to use the data for your own purposes such as marketing or solution development, you must decide these before you start collecting the data, and not collect the data for your purposes without having determined what those will be. | ← as Scenario 1<br><br>(Remember, the data is not yours to be freely used - it is regulated depending on what legal basis you are processing it with.) |
| 37 | Specificity | The purposes shall be specified and explicit as to why personal data is being processed. | Read together with 37. | ← as Scenario 1 |
| 38 | Purpose orientation | The purpose of processing should guide the design of the processing and set processing boundaries. | For example, if the purpose is solution development, consider, do you in fact need any personally identifiable data? Do you need it for that long? Do you all need access to it? And so on. | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | | If the purpose concerns of how the solution functions, ask the same questions. | |
| 39 | Necessity | The purpose determines what personal data is necessary for the processing. | (nothing to add) | ← as Scenario 1 |
| 40 | Compatibility | Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design. | Consider, how will you spot that a new processing purpose is created. Add a checkpoint in your procedures. | ← as Scenario 1 |
| 41 | Limit further processing | The controller should not connect datasets or perform any further processing for new incompatible purposes. | Add a checkpoint in your procedures, so that you can prove that you check purpose compatibility in these kinds of cases. | ← as Scenario 1 |
| 42 | Limitations of reuse | The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data. | Legitimate interest of the solution provider: If you want to use the data for your own purposes, ensure with technical and organisational measures that it is not used for other purposes within your company,<br><br>Also, consider adding technical measures in the solution that will lessen the likelihood of the employer using the data for other purposes than the solution's intended use case. Consider this as product safety measures. | - |
| 43 | Review | The controller should regularly review whether the processing is | Add a checkpoint in your procedures, so that you can prove | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | necessary for the purposes for which the data was collected and test the design against purpose limitation. | that you review purposes regularly. | |
| GDPR Principle: Data minimisation | | | | |
| 44 | Data avoidance | Avoid processing personal data altogether when this is possible for the relevant purpose. | (nothing to add) | ← as Scenario 1 |
| 45 | Limitation | Limit the amount of personal data collected to what is necessary for the purpose | (nothing to add) | ← as Scenario 1 |
| 46 | Access limitation | Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly. | See also 76-79. | ← as Scenario 1 |
| 47 | Relevance | Personal data should be relevant to the processing in question, and the controller should be able to demonstrate this relevance. | (nothing to add) | ← as Scenario 1 |
| 48 | Necessity | Each personal data category shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the | (nothing to add) | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | purpose by other means. | | |
| 49 | Aggregation | Use aggregated data when possible. | (nothing to add) | ← as Scenario 1 |
| 50 | Pseudonymization | Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately. | See ENISA guides for pseudonymisation techniques. Pseudonymisation can reduce risks considerably.<br>• https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices<br>• https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases | ← as Scenario 1 |
| 51 | Anonymization and deletion | Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted. | See about effectiveness under 65. | ← as Scenario 1 |
| 52 | Data flow | The data flow should be made efficient enough to not create more copies than necessary. | (nothing to add) | ← as Scenario 1 |
| 53 | “State of the art” | The controller should apply up to date and appropriate technologies for data avoidance and minimisation. | An example of this are self-sovereign identities and other privacy preserving technologies. | ← as Scenario 1 |
| GDPR Principle: Accuracy | | | | |
| 54 | Data source | Sources of personal data | Consider the balance between data accuracy and data | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| | | should be reliable in terms of data accuracy. | minimisation when collecting data through sensors. | |
| 55 | Degree of accuracy | Each personal data element should be as accurate as necessary for the specified purposes. | (nothing to add) | ← as Scenario 1 |
| 56 | Measurably accurate | Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence. | These may relate, tor example, to the solution identifying the person stressed or not stressed. | ← as Scenario 1 |
| 57 | Verification | Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements). | (nothing to add) | ← as Scenario 1 |
| 58 | Erasure/rectification | The controller shall erase or rectify inaccurate data without delay. The controller shall in particular facilitate this where the data subjects are or were children and later want to remove such personal data. | See 14 (privacy dashboard). | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| 59 | Error propagation avoidance | Controllers should mitigate the effect of an accumulated error in the processing chain. | (nothing to add) | ← as Scenario 1 |
| 60 | Access | Data subjects should be given information about and effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed. | See 14 (privacy dashbooard).<br>Also regard the EU Web Accessibility Directive. | ← as Scenario 1 |
| 61 | Continued accuracy | Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps. | (nothing to add) | ← as Scenario 1 |
| 62 | Up to date | Personal data shall be updated if necessary for the purpose. | (nothing to add) | ← as Scenario 1 |
| 63 | Data design | Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields. | (nothing to add) | ← as Scenario 1 |
| GDPR Principle: Storage limitation | | | | |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| 64 | Deletion and anonymizatio n | The controller should have clear internal procedures and functionalities for deletion and/or anonymization. | The solution should allow employer-initiated deletion (or anonymisation) of personal data | (nothing to add) |
| 65 | Effectiveness of anonymizatio n/deletion | The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible. | Assess the degree of anonymity that can be achieved and the risk of identification.<br><br>For anonymisation, see:<br><br>• EDPB Opinion 05/2014 on Anonymisation Techniques | ← as Scenario 1 |
| 66 | Automation | Deletion of certain personal data should be automated | Consider whether some personal data belonging to a record may be deleted earlier than other data. | ← as Scenario 1 |
| 67 | Storage criteria | The controller shall determine what data and length of storage is necessary for the purpose. | Consider each attribute if possible. | ← as Scenario 1 |
| 68 | Justification | The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question, and be able to disclose the rationale behind, and legal grounds for the retention period. | Ensure that the employer's requirements for data retention can be implemented in the solution. | Be prepared to justify the storage period to the end users. |
| 69 | Enforcement of retention policies | The controller should enforce internal retention policies and conduct tests of whether the | (nothing to add) | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | organization practices its policies. | | |
| 70 | Backups/logs | Controllers shall determine what personal data and length of storage is necessary for back-ups and logs. | Ensure that the employer's requirements for backups and logs retention can be implemented in the solution. Advice the employer as the solution provider of the technical matters relating to this, such as what can be logged. | (nothing to add) |
| 71 | Data flow | Controllers should beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their “temporary” storage. | Communicate to the employer what data flows the solution involves and what copies are created within them. | (nothing to add) |
| GDPR Principle: Integrity and confidentiality | | | | |
| 72 | Information security management system (ISMS) | Have an operative means of managing policies and procedures for information security. | Be prepared to prove to the employer who uses your solution that you have these in place. | (nothing to add) |
| 73 | Risk analysis | Assess the risks against the security of personal data by considering the impact on individuals’ rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic “threat modelling” and an attack surface analysis of the designed software | The employer using the solution is responsible for assessing risks, and the solution provider is responsible for providing all the required technical information. It is helpful to the employer if the solution provider has already carried out an assessment that the employer may refer to.<br><br>The solution provider's own assessment forms a part of its proof of being a reliable processor of the employee personal data. | (nothing to add) |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| | | to reduce attack vectors and opportunities to exploit weak points and vulnerabilities. | | |
| 74 | Security by design | Consider security requirements as early as possible in the system design and development and continuously integrate and perform relevant tests. | (nothing to add) | ← as Scenario 1 |
| 75 | Maintenance | Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing. | (nothing to add) | ← as Scenario 1 |
| 76 | Access control management | Only the authorized personnel who need to should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel. | Consider both your own personnel as well as the user roles provided in the solution. Are such roles provided that the employer can manage access to the personal data at an appropriate level? | (nothing to add) |
| 77 | -- Access limitation (agents) | Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly. | (nothing to add) | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| 78 | -- Access limitation (content) | In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee. | (nothing to add) | ← as Scenario 1 |
| 79 | -- Access segregation | Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects. | (nothing to add) | ← as Scenario 1 |
| 80 | Secure transfers | Transfers shall be secured against unauthorized and accidental access and changes. | (nothing to add) | ← as Scenario 1 |
| 81 | Secure storage | Data storage shall be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need | (nothing to add) | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br><br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br><br>Solution provider = data controller |
|---|---|---|---|---|
| | | additional security measures than others or isolation from others. | | |
| 82 | Pseudonymization | Personal data and back-ups/logs should be pseudonymized as a security measure to minimise risks of potential data breaches, for example using hashing or encryption. | Please see ENISA guides on pseudonymisation<br>• https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices<br>• https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases | ← as Scenario 1 |
| 83 | Backups/logs | Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly. | (nothing to add) | ← as Scenario 1 |
| 84 | Disaster recovery/ business continuity | Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents. | (nothing to add) | ← as Scenario 1 |

| No. | Element (EDPB) | Description (EDPB) | Guidance for Mad at Work projects - Scenario 1<br>Employer = data controller | Guidance for Mad at Work projects - Scenario 2<br>Solution provider = data controller |
|---|---|---|---|---|
| 85 | Protection according to risk | All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data. | (nothing to add) | ← as Scenario 1 |
| 86 | Security incident response management | Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches. | (nothing to add) | ← as Scenario 1 |
| 87 | Incident management | Controller should have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures, such as management of notification (to the supervisory authority) and information (to data subjects). | Ensure that you have agreed with the employer how to contact them in case there is a breach in the solution. | (nothing to add) |