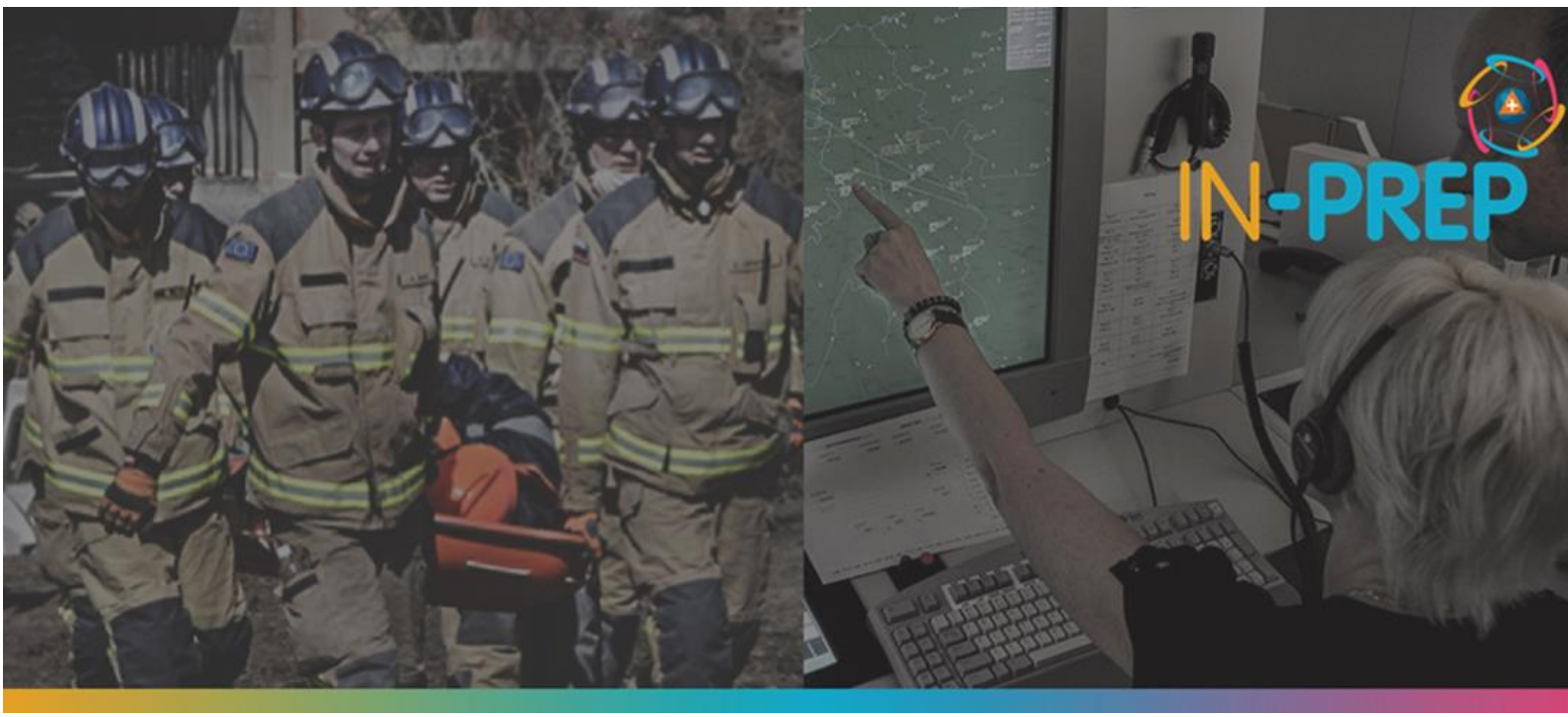
IN-PREP

"An INtegrated next generation PREParedness programme for improving effective inter-organisational response capacity in complex environments of disasters and causes of crises"

D2.3 Legal, ethical and privacy impact assessment report (Final)



This project has received funding from the European Union's Horizon 2020 innovation programme under the Grant Agreement No 740627.

Document Summary Information

Grant Agreement No	740627	**Acronym**	IN-PREP
Full Title	An Integrated next generation preparedness programme for improving effective interorganisational response capacity in complex environments of disasters and causes of crises		
Start Date	01/09/ 2017	**Duration**	36 months
Project URL	https://www.in-prep.eu		
Deliverable	D2.3, Legal, ethical and privacy impact assessment report		
Work Package	WP2 - User Needs and Ethical, Legal and Human Factors in System Development		
Contractual due date	31/08/2019 (M24)	**Actual submission date**	31/08/2019
Nature	Report ®	**Dissemination Level**	CO (Confidential)
Lead Beneficiary	TRI		
Responsible Author	Katrina Petersen (TRI, F),		
Contributions from	Primary contributors: Wendy Norris (TRI, F), Jon Betts (TRI, F), Adam Panagiotopoulos (TRI, M). All technology and end-user partners supported in the derivation of the work, even if not the writing.		

Executive Summary

This document is the final report from the ethical and privacy impact assessment in WP2 (User Needs and Ethical, Legal and Human Factors in System Development). This document is for internal use within the consortium (and towards the EC/REA) and is primarily intended to assist the consortium partners in the development and delivery of a system that meets privacy, ethical, legal, and social obligations.

This is a comprehensive report of the ethical, privacy, and legal (e.g. data protection) impact assessment process (E/PIA) conducted for the IN-PREP project. It focuses on the impact of the products produced by IN-PREP and provides recommendations for end-user requirements and the Handbook that need to be considered in order for the these products to support crisis preparedness activities that are ethical, privacy-preserving, and follow data protection and human right laws. For each risk or benefit identified, it sets out recommendations included within IN-PREP's outputs. If a recommendation is not possible in the duration of the project, it sets out considerations future end-users need to take in order to ensure their use of IN-PREP supports ethical, legal, and privacy for those that use it and those they serve through its use.

The report starts by explaining reasons for an E/PIA, the scope of the E/PIA in IN-PREP and the iterative methodology the impact assessment follows. The original methods moved from 1) identification of risks in the literature, 2) validation with external stakeholders, 3) working with partners to identify mitigation measures, 4) interviews with exercise/pilot participants, and 5) produce recommendations and end-user requirements. However, it became evident partway through the identification of mitigation measures that neither the framing of the ethical risks, the state of design, nor the technical partners familiarity with addressing ethical concerns were adequate to evaluate and validate the risks. As a result, two additional activities were devised: a) a stakeholder workshop focused on the contextual risks of transboundary technology and b) a series of semi-structured interviews with practitioners with transboundary experience. The risks and recommendations were validated through triangulation and external expert review.

Legal developments and the potential concerns that emerge from them are articulated. These focus specifically on the legal issues that affect privacy, personal data protection, ethics, and human rights. While there are many more regulations that affect IN-PREP, they are not part of the scope of this privacy and ethical impact assessment. The laws focused on are EU-level. While there are some national translations of EU regulations, a survey of the project end-users revealed that when it comes to information sharing for training and exercise purposes, their main concerns are these EU regulations. This includes: a) personal data protection regulation outside of the GDPR (e.g. the forthcoming ePrivacy regulation) pointing partners to upcoming changes they need to address to remain relevant to their market; b) non-personal data flow regulation (The Cybersecurity Act, Regulation (EU) 2018/1807, and the Open Data Directive) which require further steps within member states or certification schemes that will affect the regulatory landscape for IN-PREP's future users; c) Drone Use (EASA regulations) that standardise drone regulations across the member states, making it easier for cross-border compliance. This chapter also discusses exceptions in emergency laws that, while not immediate regulatory requirements for preparedness activities, are considerations that become relevant were IN-PREP to move into response. Considering the general end-user consensus that a training tool is only as useful as its use in response, IN-PREP risks lessening its value if it ignores these.

Data protection is directly addressed. The data protection risks are many, but the majority are low risk. This is partially due to the use of the tools under public task and the fact that the majority of the personal data gathered is about the practitioners/trainees themselves. As a result, the data protection risks focus more on the few places where incidental personal data can be gathered (e.g. chats, photos), on who are the decision makers (controllers) around personal data processing in a collaborative system, the risks towards achieving data minimisation when there are a many tools with uncertain configurations, and the risks of processing outside of the declare legal basis and purposes, all which get amplified when the data crosses between agencies. Many of the recommendations focus on the transparency needs in terms of what personal data is gathered, how it moves, what can be done with it, and what are the legally mandated documentation requirements IN-PREP has to support end-users to produce and maintain.

Privacy is considered in its more ethical sense, in contradistinction to the legal, security, and technical focus of data protection. Of specific interest to IN-PREP is behavioural privacy and surveillance. Even though

evaluation is a regular part of training, IN-PREP or not, stakeholders expressed discomfort with the thought of being surveilled in ways they are not aware. Having someone in the room with you is one thing. Having someone see only traces of your activities after the fact and make judgements raises concerns around respect, dignity, and trust. Privacy is a political move in crisis work and needs to be respected by technological design.

Ethics covers a broad range of concerns. Many of these had undercurrents around addressing diversity and avoiding bias and discrimination. In a system built on models and mock data with a focus on information sharing, the discourse consistently moved away from serving the publics, to identifying hazards and risks through shared data. While that is a major step in serving the public, the public are often missing from IN-PREP. As a result, quite a few risks and recommendations focus on how to bring those people back in to create awareness of the needs of the public(s). A second prominent thread was making the system -- including the underlying ontologies, analytics, and mixed-reality components -- transparent enough that users could understand the proportionality of their decisions, how others might understand and use the information they are providing, and avoiding liabilities, injustices, and harms that could arise from misunderstandings when working transboundary. Other ethical concerns included training towards unrepresentative mock data, accountability when managing complex systems that are not fully understood, and loss of autonomy in decision making because of a reliance on a tool that can do some of your thinking.

A few security issues emerged in relation to these topics. While by no means exhaustive to all security risks, these ones articulated emerged in relation to the risks and recommendations in the previous sections. These include risks to security from a lack of awareness or proper articulation of responsibilities and protocols when using IN-PREP, security concerns from mixing different data quality regimes, potential to combine different security standards, and the need to sometimes not share.

IN-PREP also contains micro-projects. So far, these include a triage bracelet, an embassy communication app, and – the now unlikely – facial recognition tool. These are small tools that are not part of the original project plans and do not cleanly fit within the preparedness/training framework of IN-PREP. Preliminary risks are discussed for these. Provisions for how these will follow through with the report recommendations are also provided. This section also articulates some initial concerns and benefits of including crowdtasking or social media within IN-PREP, based on interviews with practitioners with experience in doing just that.

Overall, risk trends emerged around issues of transparency (system tools, algorithmic, processing, use), the need for pre-established guidance and protocols prior to use (activities that end-users noted sometimes take years), engaging diversity and keeping the public in view, how evaluation activities can be structured to support growth and experimentation, and how IN-PREP tools for preparedness relate to the broader practices of recovery and resilience. Data protection concerns, while detailed, are low. The report ends with a description of the monitoring and evaluation procedure to take place in year three of the project.