Marie Skłodowska-Curie Actions (MSCA)
Innovative Training Networks (ITN)
H2020-MSCA-ITN-2019

Annex 1 to the Grant Agreement
(Description of the Action)
Part B

860315 – PriMa – Privacy Matters

HISTORY OF CHANGES

Version	Date	Changes
0.0	27.05.2019	Updated Table of Contents
		Added History of Changes
		Updated the ETHICS section, including the recommendations from the Ethics Screening Report
0.1	29.05.2019	To ensure consistency with the DESCA model for PriMa Consortium Agreement, Modified Section 2.3.2 as follows: *All beneficiaries agree that foreground knowledge developed in network will be owned by the beneficiaries who produced it, but other beneficiaries will be granted access rights on a royalty-free basis for internal research activities. ~~have the right to use it for research purposes~~.*
		To ensure consistency with the DESCA model for PriMa Consortium Agreement Modified Section 3.2.2 as follows: *3.2.2 Supervisory Board [..] it will comprise one representative (usually the lead researcher) from each beneficiary and partner organisation and an elected ESR representative. The SB will work as a democratic body where decisions will be presented and resolved. Each beneficiary will have a single vote, while partner organisations and the ESR representative will have an advisory function only. Decisions shall be taken by a majority of two-thirds (2/3) of the votes cast. ~~Each member will have a single vote, and if during voting a majority is not obtained, then a secret re-ballot will be conducted. If a majority is then still not obtained, the NC will cast the deciding vote.~~*

TABLE OF CONTENTS

LIST OF PARTICIPATING ORGANISATIONS

Consortium Member	Legal Entity Short Name	Academic	Non-academic	Awards Doctoral Degrees	Country	Dept./ Division / Laboratory	Scientist-in-Charge	Role of Partner Organisation
Beneficiaries								
University of Twente	UTW	√		√	Netherlands	Faculty of Electrical Engineering Mathematics and Computer Science	Raymond Veldhuis	
University of Kent	UNIKENT	√		√	UK	School of Engineering and Digital Arts	Farzin Deravi	
Norges Teknisk-Naturvitenskapelige Universitet	NTNU	√		√	Norway	Norwegian Information Security laboratory	Bian Yang	
Norsk Regnesentral Stiftelse	NRS	√			Norway	Information Security Group	Bjarte Østvold	
Julius-Maximilians Universitaet Wuerzburg	UNIWUE	√		√	Germany	Institute of Psychology	Paul Pauli	
Katholieke Universiteit Leuven	KU Leuven	√		√	Belgium	Centre for IT & IP Law	Els Kindt	
Universidad Autonoma de Madrid	UAM	√		√	Spain	Biometrics and Data Pattern Analytics (BiDA) Lab - ATVS	Ruben Vera-Rodriguez	
Partner Organisations								
GenKey Solutions B.V.	GenKey		√		Netherlands		Tom Kevenaar	Hosting secondments, member of Supervisory Board, delivering specialised training
Secunet Security Networks AG	Secunet		√		Germany		Johannes Merkle	Hosting secondments, member of Supervisory Board, delivering specialised training
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. Fraunhofer IGD	IGD		√		Germany		Andreas Braun	Hosting secondments, member of Supervisory Board, delivering specialised training
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek TNO	TNO		√		Netherlands		Paul de Jager	Hosting secondments, member of Supervisory Board, delivering specialised training
Triodos Bank NV	Triodos		√		Netherlands		Vincent Meeussen	Hosting secondments, member of Supervisory Board, delivering specialised training
Software Improvement Group B.V	SIG		√		Netherlands		Haiyun Xu	Hosting secondments, member of Supervisory Board, delivering specialised training
Callsign Inc.	Callsign		√		UK		Oscar Miguel Hurtado	Hosting secondments, member of Supervisory Board, delivering specialised training

DECLARATIONS

Name (institution / individual)	Nature of inter-relationship
TNO and UTW/Maarten Everts	TNO employee Maarten Everts is appointed as a part-time researcher (2 days/week) at UTW, who coordinates PriMa
GenKey and UTW/Raymond Veldhuis	Raymond Veldhuis (UTW) is member of the Scientific Advisory Committee of GenKey.
Callsign and UNIKENT/ Oscar Miguel-Hurtado	Oscar Miguel-Hurtado (Callsign) is a Visiting Research Fellow at UNIKENT

1. Excellence

1.1 Quality, innovative aspects and credibility of the research programme

1.1.1 Introduction, objectives and overview of the research programme

The rapid digitalisation of society, characterised by a ubiquity of sensors (in IoT and mobile devices, CCTV cameras), a high degree of interconnectivity, cloud storage, and extensive processing power, comes with increasing technology for personal information capture. Consequently, there is growing challenge to maintain individual privacy. One factor contributing to the erosion of privacy is the growth in recognition technologies that not only facilitate the recognition of individuals but also the inference from biometric data of emotional state, gender, health, age, and even profession. Another factor is fast advancement of artificial intelligence, allowing for extensive data mining, and aggregation, linkage and inference of personal information. Hence, there is a real possibility that acceptable privacy may become unattainable unless technological and societal steps are taken to allow citizens to regain control of their personal information. Therefore, *the overall objectives of the ETN PriMa are*:

1. *To train 14 creative, entrepreneurial, and innovative researchers as privacy protection experts.*
2. *To contribute to a full understanding of the multidisciplinary nature of privacy protection in a digitalised society.*
3. *To contribute to the development of solutions that address this important societal challenge.*

In support of its objectives PriMa will address a range of current issues requiring timely and societally relevant research as recently identified by OECD[1], the UN Internet Governance Forum[2], and the EU[3]. Recognising the longevity in research into privacy protection, PriMa will train a next generation of researchers to define, investigate and implement solutions that ensure secure and efficient privacy protection whilst keeping the advantages of a digitalised society, and provide them with transferable skills to enable effective planning, management and communication of research ideas and outcomes. This will give them excellent career opportunities.

PriMa will address as interrelated key themes the **analysis of privacy risks** stemming from the digitalisation of society, **protection of privacy** against these risks, and the **impact assessment** of proposed privacy protection solutions. This will be organised in three corresponding research work packages consisting of 14 inter-related projects.

1.1.2 Research methodology and approach

The research and training of the 14 ESRs will be conducted at 7 beneficiaries and 7 partner organisations, the latter comprising private research institutes, enterprises, and a bank. The training has four integral elements, providing a balance across the ETN:

1. The host beneficiary will provide resources and expertise directly associated with the ESR's project/training.
2. A secondment to another beneficiary, where the ESR will collaborate in a *paired* project, will join complementary expertise and exploit the synergy between beneficiaries.
3. A secondment to a partner organisation will provide an understanding of the current and future demands and practices regarding privacy protection, and possible integration of solutions into public and private applications.
4. Coordinated training events will the projects within PriMa and provide the ESRs with a range of transferable skills to ensure effective future research and development within the field.

PriMa will provide an original and innovative approach to a wide range of interconnected research topics, linked through the ESRs. Results will stem from joint research of experts, rather than from the aggregation of partial research activities. The cooperation between beneficiaries and partner organisations will provide a high level of applicability of PriMa's results across multiple sectors and end-users. The ESRs trained within PriMa will, therefore, be of high value to industry and society.

PriMa has organised all activities in 6 Work Packages (WPs) over 48 months, listed in Table 1.1. WP1–3 will be devoted to management, training, and dissemination, respectively, and last for the whole duration of the network. The research WPs 4, 5 and 6 will focus on the key themes: **analysis of privacy risks**, **protection of privacy**, and **impact assessment**, respectively. Research regarding ethical, legal and psychological issues is cross-cutting and will be represented in all research work packages. Each beneficiary will supervise 2 ESR projects, resulting in 14 ESR projects, each organised as a task in a research WP. Recruitment of the ESRs will start in M01 with the first research projects starting in M07. A second tranche of ESR projects will begin in M10. Each ESR project will have a duration of 36 months and will include a 4-month beneficiary secondment and a 4-month partner organisation secondment (22.2% in total). WP4—6 will commence at M07and remain active until the end of M48, allowing for a two-month

[1] http://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm
[2] https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1408
[3] https://ec.europa.eu/info/law/law-topic/data-protection_en

reporting and closure period at the end of the project. It is important to note that the work in PriMa is a series of integrated activities. The progress of each individual project will be available to all researchers, so that the results obtained by one ESR can be used by all the others. The training events (Section 1.2) are designed to stimulate and encourage cooperation. Organising the ESR projects into thematic research WPs allows for the cross-fertilisation of ideas contributing to the common goal. The WPs and deliverables are described in detail in Section 3.1.

Another accelerant for successful training and research is the pairing of ESR projects, within and across WPs, broadening the outlook for the ESRs. In pairing projects, we join complementary expertise and resources that will add to the training and exploit synergy between beneficiaries. The pairing and the joint expertise of paired projects are indicated in Figures 1.1.1 and 1.4.1.

Finally, it is of great importance that synergies appearing from the collaboration between beneficiaries, partner organisations, and ESRs are exploited and developed. Partner organisations will provide front-line information on current market and societal needs, ensuring high levels of viability and applicability of the results obtained by ESRs. They will provide career mentorship, transferable skills, experience about working in a company during secondments and contribute to the innovation-oriented mind-set that ESRs should develop during PriMa.

Table 1.1 Work Package list

WP No.	WP Title	Lead Beneficiary No	Start Month	End Month	Activity Type	Lead Beneficiary Short Name	ESRs involved
WP1	Management and Coordination	1	M01	M48	Management	UTW	-
WP2	Training and Mobility	2	M01	M48	Training, Management	UNIKENT	All
WP3	Dissemination, Standardisation, Exploitation, IPR, and Data Management	4	M01	M48	Dissemination	NRS	All
WP4	Analysis of Privacy Risks	3	M07	M48	Research	NTNU	ESR1-5
WP5	Privacy Protection	7	M07	M48	Research	UAM	ESR6-11
WP6	Impact Assessment of Privacy Protection	5	M07	M48	Research	UNIWUE	ESR12-14

1.1.3 Originality and innovative aspects of the research programme

The research in PriMa is beyond the state of the art as it introduces novel methods to analyse privacy risks, novel approaches to privacy protection, and new insights in the vulnerabilities of, for instance, biometric data, data sharing and mining, blockchain-based data markets, and modern finance applications. In particular, PriMa's novelty is in the introduction into privacy analysis and protection of new technologies such as machine and deep learning, homomorphic encryption, self-sovereign identity management, and blockchain. It is the first MSCA-ITN to analyse the impact of privacy protection by means of virtual reality and to develop technological tools for checking compliance with legislation. Additionally, PriMa has an original structure with paired projects, secondments that are balanced between research and application, and focussed training events. PriMa builds on results of previous EU projects in biometrics and privacy such as 3DFace, TURBINE, PRIME, TABULA RASA, PRIMELIFE, and AMBER, which have addressed and provided groundwork on parts of PriMa's thematic area.

The relations between the research work packages and the pairing of ESR projects across and within work packages are shown in Figure 1.1.1. The partner secondments are further detailed in Figure 1.4.1. The pairing of ESR projects is aimed at joining complementary expertise in the areas: quantifying privacy; policy checking of novel solutions; profiling and counter measures, machine learning based privacy analysis and protection (linking WPs 4 and 5); privacy regulation and user behaviour (linking WPs 4 and 6); user acceptance of privacy protected services, social contract-based privacy and legislation

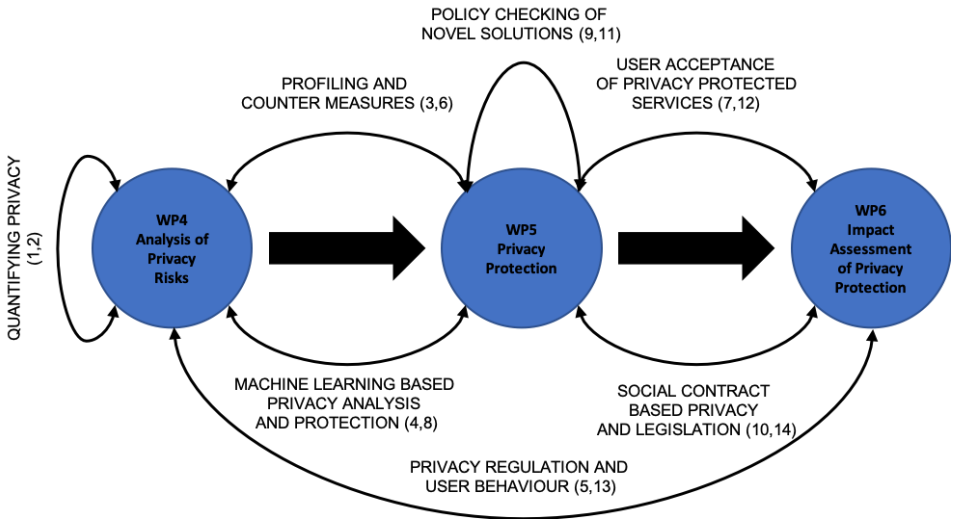

Figure 1.1.1 Dependencies between work packages and paired projects. The numbers indicate the ESR projects.

(linking WPs 5 and 6). The content of the research WPs and the ESR projects is presented below. As will be detailed throughout this proposal, the major novelties in the design and execution of the network are:

- The integrated treatment of psychological, legal and ethical subject areas inside the research WPs.
- Paired ESR projects, joining complementary expertise and a beneficiary secondment at the paired project's beneficiary.
- A consistent design of ESR projects, each with one industrial and one academic secondment, timed such that they have maximum impact on training.
- Consecutive beneficiary secondments of paired projects, such that the ESRs involved can spend 8 months working physically together on a joint subproject.
- Assigning an industrial mentor to each ESR, guiding him or her in the development of transferable skills.
- High impact of results through interaction with standardisation bodies, government and industry.
- Input from a range of leading experts in the field.

WP4: Analysis of Privacy Risks. The goal of this research WP is to conduct research beyond the state of the art on methods for privacy sensitivity assessment of upcoming and established biometric modalities and for the analysis of privacy risks of cloud storage and processing and other activities on the internet. ESR projects 1-4 involve technical research aiming at the assessment of privacy risks. ESR project 5 considers legal aspects of privacy risks.

ESR1: Quantifying Privacy with Application to Emerging Biometrics (UAM). Technological evolution has enabled smartphones to acquire huge amounts of different sources of information. Some are traditional biometrics such as fingerprint or facial images, but additionally other sources can be used to extract information about the user as well, such as touch gesture patterns, soft biometrics[4,5] (age, gender, etc.), movement patterns from the accelerometer sensor, or context information[6,7,8,9] (patterns of apps usage, transactions, etc.). The combination of these sources of information could be used to generate a profile of the user containing sensitive information. This project will focus on quantifying privacy in the context of data acquired through the interaction of the user with the technology following a theoretical and practical approach as current schemes to quantify user privacy in this context have limitations[10,11,12]. **The scientific goal of this ESR project is** to build upon a systematic evaluation of existing methods to produce better methods to quantify privacy and evaluate their effectiveness for emerging applications.

ESR2: Mobile Device Background Sensors: Authentication vs Privacy (UNIKENT). Conventional protection of mobile devices requires the authentication of the user only at the start of the device interaction. To prevent unauthorised usage during runtime, the user can be continuously re-authenticated by the system, with the potential to simplify and enhance levels of authentication and convenience to the user. Behavioural/temporal characteristics of device use can be used for continuous authentication[13]. However, collecting data raises issues concerning the privacy of the individual and information misuse. Modern smartphones and tablets have many sensors, and there is a considerable amount of data that can be collected and used for continuous authentication. Examples include GPS location, Wi-Fi cell/mast location, gyroscope/accelerometer movement, and light and temperature, alongside patterns of device usage. A number of studies have assessed the use of these data both individually and in combination with conventional security systems. Different usage characteristics can be assessed from direct device interaction including hand movements, orientation, and grasp[14,15]. Using continuous authentication may also bring limitations: accuracy can require high energy consumption and often a long training time[16]. Research in the field is very much

[4] P. Samangouei et al., "Facial Attributes for Active Authentication on Mobile Devices", Image and Vision Computing, 2016.

[5] E. Gonzalez-Sosa, et al., "Facial Soft Biometrics for Recognition in the Wild: Recent Works, Annotation and COTS Evaluation", IEEE Trans. on Information Forensics and Security, Vol. 13, n. 7, 2018

[6] V. Patel et al., "Continuous user authentication on mobile devices: Recent progress and remaining challenges", IEEE Signal Processing Magazine, 2016.

[7] Y. Montjoye, et al., "Unique in the shopping mall: On the reidentifiability of credit card metadata" Science, Vol. 347, Issue 6221, pp. 536-539, January 2015.

[8] T. Neal et al., "Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits," in IEEE International Conference on Biometrics Theory, Applications and Systems, Sept 2015, pp. 1–6, 2015.

[9] F. Li et al., "Active authentication for mobile devices utilising behaviour profiling," Int. Journal of Information Security, vol. 13, no. 3, pp. 229-244, 2014.

[10] C. Lee, Y. Guo, L. Yin, "A Framework of Evaluation Location Privacy in Mobile Network", Procedia Computer Science, Volume 17, 2013, Pages 879-887.

[11] Rehman, Muhammad Habib ur et al. "Mining Personal Data Using Smartphones and Wearable Devices: A Survey." Sensors (Basel, Switzerland) 15.2 (2015): 4430–4469. PMC. Web. 1 Dec. 2017.

[12] H. Li et al. "URLSight: Profiling Mobile Users via Large-Scale Internet Metadata Analytics," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 1728-1733.

[13] Kim B. Schaffer, "Expanding Continuous Authentication with Mobile Devices", Computer, vol. 48, no 11, pp. 92-95, Nov. 2015, doi:10.1109/MC.2015.333

[14] Z. Sitova et al., "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users", IEEE Trans. IFS, PP(99): 1-1,2016

[15] L. Fridman et al. , "Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location," IEEE Systems Journal, pp. 1–10, 2015.

[16] D. Buschek, A. De Luca, and F. Alt, "Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2015, pp. 1393–1402

in its infancy and, whilst levels of convenience might be enhanced, understanding the privacy issues of continuous data reporting needs research and exploration. **The scientific goal of this ESR project is** to evaluate the performance and privacy of continuous biometric authentication background sensors and methods on mobile devices. Background sensors include accelerometers, gyroscopes and GPS/Wi-Fi network location. Our study will evaluate the data richness of these sensor changes, balancing biometric performance against privacy issues

ESR3: Biometric profiling of facial images and templates (UTW). Raw biometric data contains more than just identity information. Recent research has shown that not only age, gender, and ethnicity can be inferred from a facial image but also profession (e.g. is a CEO or a professor[17]) or the probability of being a criminal[18]. It is expected that other attributes can be inferred as easily by training a classifier for that purpose. This brings the risk of unwanted biometric profiling either on facial images stored in a database or on the multitude of images available on the internet. Although the templates of state-of-the-art face recognition systems, including those based on deep learning, are designed to contain discriminative identity information only, it can be assumed that they contain information about other attributes and hence are privacy sensitive. **The scientific goal of this ESR project is** to analyse and mitigate the risk of biometric profiling on facial images and templates. It will investigate: (1) The risk of biometric profiling by attributes that can be inferred from facial images and (2) from templates. (3) The characteristics of the face and of templates that contribute to profiling. (4) Methods to reduce the risk of profiling.

ESR4: **Modelling Private Identity Management Behaviours by Digital Footprints (NTNU).** How a person manages his/her private identities (e.g., setting up and changing account names and passwords, choosing identity providers) can be heavily influenced by the person's knowledge scope, personality, body characteristics, and life patterns, which can already partially be traced as digital footprints online[19] and will be even more exposed in future through the Internet of Things. We assume that the cumulative character of digital footprints will enable correlation analysis between people's personal information[20] and their private identity management behaviours, and in turn will endanger the privacy of the identity principals and the security of associated identity management methods. This can be even more complicated in multi-party scenarios[21] and creates a serious challenge to the future trend of self-sovereignty identity management. **The scientific goal of this ESR project is** to test this assumption, by quantifying the relations between digital footprints and identity attributes and modelling these by statistical and machine learning methods. Particular attention will be paid to the dynamics of human behaviour in identity management under various scenarios (e.g. password changing, mnemonic password construction, honey templates generation[22], consent giving in private/public scenarios) before and after receiving privacy and security awareness training. To collect data for research and performance evaluation, social communication mechanisms in real life such as social network and social robot are planned to be utilised to test the models by a series of announced and unannounced experiments compliant to the requirements of the General Data Protection Regulation (GDPR)[23].

ESR5: Privacy and biometrics in health and activity tracking (KU Leuven). Consumer-grade fitness and activity tracking devices, attached to a subject's wrist and packed with sensors ranging from simple accelerometers and gyroscopes to galvanic skin response and optical heart rate monitors, constantly collect a broad catalogue of health-related personal data from their users.[24,25] With the advent of quantum computing, anonymization techniques applied to data collected by these devices will no longer meet the legal concept of anonymity. The logical question arises of whether true anonymization would be at all possible in the near future[26] and what would be the legal response. If true anonymization is at risk, research is required into identifying whether the law has to consider new avenues to mandate protection of these personal data. The principle of finality of purposes is also put to the test by the possibilities revealed by these devices.[27] With questions varying from whether these personal data could be

[17] J.I. Stoker et al., "The Facial Appearance of CEOs: Faces Signal Selection but Not Performance". PLos ONE, 11 (7). e0159950:1-11, 2016, ISSN 1932-6203
[18] X. Wu, X. Zhang (2016) "Automated Inference on Criminality using Face Images", https://arxiv.org/abs/1611.04135
[19] R. Lambiotte and M. Kosinski, "Tracking the Digital Footprints of Personality," *Proceedings of the IEEE*, Vol.102, no.12, Dec. 2014.
[20] Y. Li, H. Wang, and K. Sun, "A study of personal information in human-chosen passwords and its security implications," *IEEE INFOCOM* 2016.
[21] J. Such and N. Criado, "Multiparty Privacy in Social Media," Communications of the ACM, August 2018, Vol. 61 No. 8, Pages 74-81
[22] B. Yang and E. Martiri, "Using Honey Templates to Augment Hash Based Biometric Template Protection," *IEEE COMPSAC* 2015.
[23] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.
[24] S.R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85, 101–02 (2014).
[25] Steven Spann, Wearable Fitness Devices: Personal Health Data Privacy in Washington State, Seattle UL Rev. 39, 1411 (2015).
[26] Jennifer Chu, The beginning of the end for encryption schemes? MIT News, available at: http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303.
[27] Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, p. 7.

stored in public or cloud environment[28] through their potential role in remote clinical trials[29], to their use by third party applications installed on these devices, the purpose limitation principle seems to be an insufficient tool to deal with the different interests of the involved parties. In light of the (in)security brought by the newly adopted Privacy Shield, transfers of personal data outside the EU could be clouded by even further uncertainty. Many of these devices' capabilities could be easily extended by means of third-party applications.[30] These applications may involve multiple international data transfers between different parties which makes it exceedingly difficult to clearly distinguish between controllers and processors. Finally, these devices are likely capable of making inferences of a person's health based on collected behavioural biometrics data. It remains to be seen to what extent and in what circumstances, if at all, such inferences based on collected behavioural biometric data could be considered legally sound. **The scientific goal of this ESR project is** to perform research into identifying whether the law has to consider new avenues to mandate protection of personal data gathered by health and activity tracking devices.

WP5: Privacy Protection. Based on the analyses of WP4, the goal of this WP is to develop methods to mitigate privacy risks, including prevention of unwanted biometric recognition, protection of biometric data, and the use of blockchain technology in self-sovereign identity management. ESR projects 6—9 aim at solutions to known privacy risks, whereas ESR project 10, and even more so ESR project 11 aim at the design of systems and software compliant to privacy protection regulations and directives.

ESR6: Biometric Identity Hiding, Obfuscation and De-identification (UNIKENT). With the proliferation of mobile devices with built-in sensors and advances of data sharing and social networks, including the storage of meta data regarding each interaction, often without explicit knowledge or permission, the potential for severe erosion of privacy is on the rise. This has resulted in a greater need for protection against unwanted biometric data capture. Ideally such protection should take place as early as possible in the processing chain to minimise the potential for privacy being compromised. Moreover, it is desirable to provide users with the means to control the acquisition of their identity-revealing information at the sensor level of biometric systems by themselves. In this way, they do not need to rely on the unknown or unverified privacy features of devices and systems that they do not control. There has been an emerging interest in technologies that may prevent the capture and processing of biometric data. Examples of these include the use of head-wear and makeup[31] as well as projected illumination[32] to prevent face detection and recognition. It may also be possible to envisage systems that remove the biometric data after capture using a process called de-identification[33]. Given a robust legal-framework it may be possible for data-subjects to indicate their wish for privacy and the biometric systems to take action to immediately remove biometric data during capturing thus ensuring privacy protection. However, the performance and effectiveness of these technologies have not been fully evaluated against the increasing more powerful techniques for biometric recognition based on increasing processing power and the progress in machine learning[34,35]. More research needs to be done to establish the capabilities and limits of such systems and to investigate the potential of new technological developments. **The scientific goal of this ESR project is** to develop and evaluate the effectiveness of new and emerging technologies for privacy protection at the sensor-level.

ESR7: Identity provisioning in the cloud: Privacy, security, and user experience when authenticating to services (NRS). Our digital milieus are rich and detailed. Sensors in, for example, smartphones, cars, and Internet of Things devices, continuously collect biometric data and other data about us. This data is voluminous and personal since it concerns our appearance, behaviours, and habits, thus allowing for continuous authentication[36,37]. The objective of the project is to describe how privacy, security and user experience are affected by design choices when building

[28] Ibid. 8.

[29] PwC Health Research Institute, Health wearables: Early days, p. 1, available at: https://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/pwc-hri-wearable-devices.pdf. See also Christina Farr, Exclusive: Two Apple medical trials shed light on how HealthKit will work, Reuters, http://www.reuters.com/article/2014/09/15/us-apple-health-idUSKBN0HA0Y720140915, Sept. 15, 2014.

[30] K. Britton, IoT Big Data: Consumer Wearables Data Privacy and Security, ABA Section of Intellectual Property Law, p. 1, available at: http://www.americanbar.org/content/dam/aba/publications/landslide/2015-november-december/ABA_LAND_v008n02_iot_big_data_consumer_wearables_data_privacy_and_security.authcheckdam.pdf.

[31] R. Fen and P. Balakrishnan. "Facilitating fashion camouflage art." Proceedings of the 21st ACM international conference on Multimedia. ACM, 2013.

[32] T. Yamada et al., "Privacy visor: method for preventing face image detection by using differences in human and device sensitivity." IFIP International Conference on Communications and Multimedia Security. Springer Berlin Heidelberg, 2013.

[33] S. Ribaric, et al. "De-identification for privacy protection in multimedia content: A survey." Signal Processing: Image Communication (2016).

[34] Wilber, M et al., "Can we still avoid automatic face detection?." 2016 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE, 2016.

[35] H. Rashwan, et al. "Defeating face de-identification methods based on DCT-block scrambling." Machine Vision and Applications 27.2 (2016): 251-262.

[36] Ibid 6.

[37] Ryan Johnson, et al., "Pairing continuous authentication with proactive platform hardening: PerCom Workshops 2017: 88-90.

services that use cloud-based identities and also when constructing the identity provisioning itself[38]. Such choices include what personal data to collect and how and where to process and store it and how to manage and mitigate privacy risks in such services. Identity providers want to know users' entire digital milieu to better identify them and to let users authenticate passively, while users have privacy concerns. Project topics include formal modelling, secure authentication, security of cloud-based services, advanced data analysis and its effect on privacy, and the relation between privacy, user experience and security. **The scientific goal of this ESR project is** to identify the core the principles of such identity provisioning, and based on that, enabling a sound method for designing systems involving identity provisioning.

ESR8: Privacy Protection in Multimodal Biometrics with Application to e-Learning and e-Banking (UAM). This project will consider privacy protection for multimodal biometric systems in the context of two case studies of great interest for biometrics: e-Learning and e-Banking. e-Learning is an exponentially growing field, with the main MOOC platforms claiming over 34 Million students in 2017. Numerous techniques have been proposed for biometric template protection over the last 20 years, mostly for unimodal biometric systems. While these techniques are theoretically sound, they seldom guarantee the desired non-invertibility, revocability, and non-linkability properties without significantly degrading the recognition performance[39]. This limitation can be overcome by introducing multi-biometric template protection schemes[40], since the combination of different biometric characteristics generally leads to higher accuracy[41]. Even though extensive research has been carried out on the fields of multi-biometric recognition and unimodal biometric template protection[42], several issues remain unsolved in the development of multi-biometric template protection schemes[43,44,45]. **The scientific goal of this ESR project is** to address two of the most significant challenges[46], in particular: 1) the development of a generic framework for multi-biometric template protection, and 2) the difficulty to obtain protected templates from non-pre-aligned samples, without requiring auxiliary data (and hence avoiding potential information leakage).

ESR9: Integration of biometric recognition and homomorphic encryption (UTW). Established measures for privacy protection of stored biometric templates are (1) the classical template protection methods such as helper-data systems[47] and (2) the more recent methods that perform biometric recognition under encryption[48]. The first have the advantages that no key management is required, and computational complexity is low. The disadvantage is that the strength of the privacy protection is fully determined by the recognition performance of the biometric modality and for known modalities the secrecy rate does not exceed more than 20 bits, which is marginal from a cryptographic point of view[49]. In the second approach the protection of privacy is decoupled from the biometric recognition performance and depends on the strength of the encryption, but this requires significant computational resources. Recent research has shown that a novel approach integrating the optimal likelihood-ratio-based classifier in a homomorphic encryption scheme results in a very fast biometric recognition under encryption with near optimal recognition performance[50]. The approach works in a 2-party scheme where a client contains the biometric sensor and the templates are stored on a server. It is secure in an honest-but-curious setting. **The scientific goal of this ESR project is** to develop this approach further. In particular, it will investigate: 1) The pre-processing and conditioning of biometric features of state-of-the-art biometric recognition systems, including those based on deep learning, so that they can work with a homomorphically encrypted likelihood-ratio-based (HELR) classifier. 2) Extension to other multi-party schemes and relaxation of the honest-but-curious requirement.

---

[38] J. Bringer et al., Privacy by Design in Practice: Reasoning about Privacy Properties of Biometric System Architectures, Int. Symp. on Formal Methods, 2015.

[39] K. Nandakumar and A. K. Jain. "Biometric template protection: Bridging the performance gap between theory and practice". IEEE Signal Processing Magazine, 32(5):88–100, 2015.

[40] A. Nagar, et al.. Multibiometric cryptosystems based on feature-level fusion. IEEE Trans. on Information Forensics and Security, 7(1):255–268, 2012.

[41] A. Ross, K. Nandakumar, and A. Jain. Handbook of Multibiometrics. Springer, 2006.

[42] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(3).

[43] C. Rathgeb and C. Busch. New Trends and Developments in Biometrics, chapter Multi-biometric template protection: Issues and challenges. InTech, 2012.

[44] M. Gomez-Barrero, et al, "Unlinkable and irreversible biometric template protection based on Bloom filters", Information Sciences, Vol. 370-371, pp. 18-32, November 2016.

[45] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi and J. Fierrez, "Multi-Biometric Template Protection Based on Homomorphic Encryption", Pattern Recognition, Vol. 67, pp. 149-163, July 2017.

[46] M. Gomez-Barrero, "Improving Security and Privacy in Biometric Systems", PhD Thesis, Universidad Autonoma de Madrid, Spain, June 2016

[47] J. Breebaart, et al. "A reference architecture for biometric template protection based on pseudo identities" in *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, September 11-12, 2008, LNI-Series.

[48] J. Bringer, et al. "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends", IEEE Signal Processing Magazine, 30(1):42–52, 2013.

[49] R. Veldhuis. "The relation between the secrecy rate of biometric template protection and biometric recognition performance" in *ICB 2015*, pp. 311-318, May 2015.

[50] J. Peeters, et al. Fast and Accurate Likelihood Ratio Based Biometric Comparison in the Encrypted Domain. arXiv preprint arXiv:1705.09936, 2017.

ESR10: Multi-party social contracts and privacy mechanisms (NTNU). The trend of personalised digital services inspires us to look for new models for definitions and legislations regarding privacy. The social contract[51] approach is a promising concept to model privacy in a future of personalised digital services from the perspective of cross-party rights and duties provenance and computational negotiation instead of trying to define information ownership. However, there are uncertainties in the legal, ethical, and technological aspects of implementing this concept in practice. The ESR will be trained to master the knowledge and skills in e.g., social contract methodologies, risk management, multi-party privacy, privacy-preserving methods, computational negotiation, self-sovereign identity management, and will become an expert in the social contract approach to model privacy. **The scientific goal of this ESR project is to** evaluate the feasibility using social contract to model privacy in the future, by answering the following questions: (1) Is it viable to model privacy by social contract in harmony with existing law or directives such as the General Data Protection Regulation (GDPR)[52], and the Payment Services Directive (PSD 2)[53], and future legislation process and how to do this? (2) How to technologically enable the social contract concept in a secure and privacy-preserving way, and how to construct a trustworthy cross-party automated rights negotiation mechanism. (3) Will such social contract-based privacy personalisation models cause ethical and societal challenges (e.g., social inequality) and how to mitigate these risks?

ESR11: Detecting privacy problems in software (NRS). EU's new data protection law, GDPR[54], was implemented in May 2018 with fines up to 4% of the annual turnover of a service. **The scientific goal of this ESR project is to** perform research on methods that help software development organisations write software that complies with the new regulation, supporting privacy by design[55,56] of software. The work will build on previous work on formal specification (e.g., the Java Modelling Language) and existing tools for property checking and analysis of software and protocols[57,58,59,60]. The project shall extend and adapt these techniques to discover defects and design flaws related to personally identifiable data and privacy policies, including the treatment of biometric information in distributed systems, including flaws related to the assessed privacy impact of software. The project will also consider how to support the development process, e.g., mediate interaction between developers and generate privacy-related unit tests. Key sources of inspiration are the body of work on finding security defects in software and analysing cryptographic protocols and work on privacy by design. Project topics include privacy engineering[61] and its relevance for software development, formal specification, and static analysis.

WP6: Impact Assessment of Privacy Protection. The best privacy protection will be ineffective if not accepted by users and society and not applied in daily life. Therefore, the goals of this work package are to assess the impact and viability of privacy protection technologies such as developed in WP5 and to ascertain how they have to be refined to improve the user's and societal acceptance without undermined social rules of communication.

ESR12: Acceptance and usage of privacy protection solutions (UNIWUE). A user's behaviour may be motivated, on the one hand, by reflections on long-term outcomes based on knowledge, but on the other hand, by an emotional impulse to reach the desired goal immediately without considering long-term consequences, social influences, or instructions[62,63]. Thus, consumer acceptance, usage and usability of any privacy protection solution may vary considerable depending on cognitive and social factors as well as the user's emotional state. This project will examine ways to improve acceptance, usage and usability of data protection solutions in daily life and under typical emotional states (e.g. stressful office situation, relaxed home situation, public meeting, private meeting) induced by virtual reality[64]. The user will be immersed in typical virtual situations and be confronted with privacy protection or

[51] K. Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," Journal of Business Ethics, 137(3), pp 551–569, September 2016.
[52] Ibid 23.
[53] Payment services (PSD 2) - Directive (EU) 2015/2366. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[54] Ibid 23.
[55] T. Antignac, D. Le Métayer. Trust Driven Strategies for Privacy by Design, Trust Management IX: 9th International Conference, IFIP WG 11.11, 2015.
[56] S. Joyee De, D. Le Métayer, "Privacy Risk Analysis. Synthesis Lectures on Information Security, Privacy, & Trust", Morgan & Claypool Publishers 2016.
[57] F. Nielson et al., Principles of Program Analysis, Springer, 1999.
[58] https://find-sec-bugs.github.io/
[59] https://www.owasp.org/index.php/Static_Code_Analysis#Tools
[60] http://findbugs.sourceforge.net/, http://fbinfer.com/
[61] Seda Gürses and Jose M. del Alamo, Privacy Engineering: Shaping an Emerging Field, of Research and Practice, IEEE Security & Privacy 14(2): 40-46 (2016).
[62] Y. Shiban, et al. The Appearance Effect: Influences of virtual agent features on performance and motivation. Computers in Human Behavior, 49, 5-11, 2015
[63] M. Kinateder, et al. Social influence in a virtual tunnel fire – Influence of conflicting information on evacuation behavior. Applied ergonomics, 45(6), 1649-1659, 2014
[64] Dobricki, M. & Pauli, P. (2016). Sensorimotor body-environment interaction serves to regulate emotional experience and exploratory behavior. Heliyon, 2, e00173. doi: 10.1016/j.heliyon.2016.e00173

surveillance equipment. The behaviour as well as cognitive and emotional responses will be analysed in order to allow conclusions about improvement of acceptance, usage, usability, e.g. on the basis of instructions[65]. **The scientific goal of this ESR project is** to develop and use innovative ecologically valid approaches to evaluate and improve consumer acceptance, usage and usability of privacy protection solutions.

ESR13: Privacy protection effects on social communication (UNIWUE). Technology changes social communication in a way that direct personal contact decreases while technology-mediated communication increases. Thus, a user can create an optional picture of himself and even an avatar for communication, and this may affect emotional responses[66]. This may help to protect privacy, but simultaneously may lead to anonymity that may dismantle social rules and restrictions. This project will examine how changing communication from surveillance to privacy and to anonymity will affect communication behaviour. **The scientific goal of this ESR project is** to develop and evaluate technological solutions that on the one hand guarantee anonymity and privacy protection but on the other hand prevent violations of social rules and other unwanted effects.

ESR14: Legal digital identity: reconciling blockchains, biometrics and privacy (KU Leuven). Blockchain-based systems are seen as enablers of the creation of a legal digital identity for all individuals.[67] An initial identity record could be made on a blockchain upon individual's birth with information for relevant life events being added later in time.[68] Legal research is needed to clarify how to authenticate the owner of a particular record on the blockchain and whether the solution in the development of a system based on dynamic biometrics is viable. Relying on the 'sensor world' we live in, such a system could be based on two or more behavioural biometrics by connecting, for example, heart rate, movement, and location by means of smart devices (smartphone, body monitor and a smart watch).[69] Although combining blockchain with biometrics seems to put users in control, there are growing concerns that the new GDPR[70] is not fit for the distributed peer-to-peer architecture of the blockchain involving multiple (personal) data transfers, making it extremely difficult to determine the 'classical duo' of controller(s) and processor(s).[71] Furthermore, the exercising of individuals' rights to erasure and modification of their personal data might be endangered by the irreversibility and transparency created by blockchains.[72,73] Some see the combining of biometrics' irrevocability and blockchains' immutability as an immense danger in dealing with compromised biometrics. Others believe that with the user being the weakest point in a blockchain, by creating a 'biometric password' she becomes the owner of her data for life. In this view, by storing their biometric data cryptographically across multiple computers, users are protected against interference of malicious third parties.[74] Legal research is required to assess the viability of these solutions. Furthermore, considering the sensitivity of biometric data, the law is facing difficulties in reconciling the inherently immutable nature of the blockchain with the benefits of biometrics and the right to privacy. In legal terms, a solution should be sought that aims to take 'the best of both worlds' while still keeping individuals' fundamental rights high on the agenda. **The scientific goal of this ESR project is** to perform legal research to assess the viability of solutions based on blockchain and biometrics, considering the sensitivity of biometric data, the inherently immutable nature of the blockchain, and the right to privacy.

1.2 Quality and innovative aspects of the training programme

1.2.1 Overview and content structure of the training (ETN)

At present, there are no academic programs that aim at the education of privacy protection experts. Present research in this field is mainly mono-disciplinary, either technical, legal, or psychological with insufficient focus on societal impact. The training in PriMa will provide useful and valuable transferable knowledge for all ESRs to suc-

[65] A. Mühlbergeret al. Influence of Information and Instructions on Human Behavior in Tunnel Accidents: A Virtual Reality Study. Journal of Virtual Reality and Broadcasting, 12 (3), 1-13, 2015

[66] Cheetham, M. et al. (2015). Arousal, valence and the uncanny valley: psychophysiological and self-report findings. Frontiers in Psychology, 6.

[67] Yorke Rhodes III, What does identity mean in today's physical and digital world? Microsoft Azure Blog, available at: https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital-world.

[68] Gunnar Nordseth, Blockchain: identity revolution or evolution? Signicat, available at: https://www.signicat.com/eid/blockchain/.

[69] Jennifer Langston, Secure passwords can be sent through your body, instead of air, University of Washington Today, available at: http://www.washington.edu/news/2016/09/27/secure-passwords-can-be-sent-through-your-body-instead-of-air/.

[70] Ibid 23.

[71] Jason Albert, What's Next for Blockchain: Technology, Economics and Regulation, Microsoft EU Policy Blog, available at: https://blogs.microsoft.com/eupolicy/2016/06/20/whats-next-for-blockchain-technology-economics-and-regulation/.

[72] Jeni Tennison, What is the impact of blockchains on privacy? Open Data Institute, available at: https://theodi.org/blog/impact-of-blockchains-on-privacy.

[73] Giuseppe Ateniese et al., Redactable Blockchain–or–Rewriting History in Bitcoin and Friends, (2016), available at: http://eprint.iacr.org/2016/757.pdf.

[74] Julia Daimio, Together We Stand: Will Biometrics and Blockchain Build a Joint Future? The Cointelegraph, available at: https://cointelegraph.com/news/will-biometrics-&-blockchain-build-a-future.

cessfully undertake future activities that are relevant to future developments and initiatives regarding privacy protection. The training with PriMA comprises three components delivered at a local or network-wide level:

a) *Research Training (Project-Specific) for each ESR delivered by the host and secondment institutions (local)*,
b) *Research Training (Network-Wide) providing academic and technical exposure to the multiple disciplines within PriMa – delivered at Network Training Events (network-wide), and*
c) *Transferable Skills Training – delivered to individual ESRs at host and secondment institutions, and at network training events (local and network-wide).*

Each component is described in detail in this section in relation to the central themes and objectives of PriMA. Our underlying ethos in research training is the promotion of inter- and multi-disciplinary research to provide the EU with experts, able to advance the state-of-the-art in privacy protection in a digitalised society, placing Europe in a strong leadership position within the global market. Importantly, PriMa will provide training in transferable skills to support ESRs to obtain relevant positions within industry or academia upon completion.

Training Management: Development and monitoring of training within PriMa will be coordinated through WP2 led by UNIKENT, who will report directly to the Supervisory Board. *Local* training (both Research and Transferable Skills training) will be delivered by the individual beneficiaries, secondment beneficiaries and partners organisations, tailored to the individual ESR projects. Each ESR project will be assigned to one of the three research WPs covering PriMa's key themes: **analysis of privacy risks**, **protection of privacy**, and **impact assessment**. Each WP consists of 3 to 6 complementary ESR projects from different institutions and will be led by a beneficiary, who is a senior academic expert in the thematic area, and who will be responsible for ensuring an appropriate level of research training across the ESRs within a WP. Each WP leader will report to the lead of WP2 regarding progress of the local research and transferable skills training. The production and organisation of *network-wide* research and transferable skills materials including a series of network training events will be tasks of WP2. WP2 will use the first months, before the ESRs have formally commenced their secondment, to define common materials for training, building and assimilating from best practice across the consortium members

The ESRs: The 14 ESRs will primarily participate in the PhD programmes of their host beneficiary institutions. When not on secondment, they will work at their host institutions, with regular communication with the other ERSs in PriMa (electronic or otherwise). Twice per year they will meet physically at PriMa's Training Events which comprise of 3 *Research Events* and 3 *Workshops*. Each Research Event will be themed aligned to a particular technical WP(s). In a Research Event, all ESRs will report on progress within their projects and work together on the Research Event theme, thus extending the training beyond the theme of the ESR's own WP. This joint work will be coordinated by the WP leader and the ESRs of associated WP, thus developing transferable skills regarding teamwork and project management. This integrated work will help to realise global research outcomes per WP that are applicable to a variety of applications and, with the involvement and help of PriMa's partner organisations, directly transferable to industry and society. Results from the projects and Events will be disseminated according to PriMa's dissemination policy (Section 2.3). ESRs, hosts, WPs and paired projects are shown in Table 1.2a. Workshops will focus on the training of network-wide transferable skills as well as update all ESRs on recent progress. The events are described in detail in Table 1.2b.

Table 1.2a Recruitment Deliverables per Beneficiary

Researcher No.	Recruiting beneficiary	Planned Start Month	Duration (months)	WP	Paired project	Researcher No.	Recruiting beneficiary	Planned Start Month	Duration (months)	WP	Paired project
ESR1	UAM	7	36	4	ESR2	ESR8	UAM	10	36	5	ESR4
ESR2	UNIKENT	10	36	4	ESR1	ESR9	UTW	7	36	5	ESR11
ESR3	UTW	10	36	4	ESR6	ESR10	NTNU	10	36	5	ESR14
ESR4	NTNU	7	36	4	ESR8	ESR11	NRS	10	36	5	ESR9
ESR5	KU Leuven	10	36	4	ESR13	ESR12	UNIWUE	10	36	6	ESR7
ESR6	UNIKENT	7	36	5	ESR3	ESR13	UNIWUE	7	36	6	ESR5
ESR7	NRS	7	36	5	ESR12	ESR14	KU Leuven	7	36	6	ESR10

Training Implementation: The training of the ESRs consists of a well-balanced mix of Network Training Events, supervised research at host and secondment institutions, complemented with local courses at host and secondment institutions. The Career Development Plan (CDP) of an ESR describes the training of the ESR in detail, including mobility aspects and expected academic output in terms of publications and deliverables. Each of the beneficiaries will enrol their hosted ESRs on an institutional PhD programme, which will become an integral part of the CDP.

Although varied across beneficiaries, common elements of institutional PhD programmes include a variety of transferable skills courses, including generic scientific research and dissemination practice, ethical issues, presentation skills, experimental design, background literature surveying and academic reporting writing. ECTS points awarded for a training course offered by an external institution will be accepted by the host institution. The specific implementation of research and transferable skills training are described below in relation to PriMa's objectives. As mentioned, each ESR will receive research and transferable skills training. This will vary considerably from project-to-project but will include subjects such as data analysis, classifier design, statistics, sociological and psychological theory, programming, legal analysis, data security technologies, and discipline-specific results presentation, documentation and communication.

Research Training: The primary goals of the research training are to provide the ESRs with the necessary research skills that will enable them to work as a privacy protection specialist, and to enable them to obtain a PhD at their host institution. Research training will be achieved through the following mechanisms:

- Active research: Each ESR will work on a well-defined research topic with specific objectives and target dates, under guidance of an academic supervisor (Obj. 1, Section 1.1.1). Their work will start with studying the state-of-the-art in their field and setting up a detailed research plan. This will be executed at both the hosting institution and through secondment at other participants of the network (Obj. 3). Research interaction within PriMa will be achieved using the thematic WP training during the Network Training Events and the joint work during the secondments as well as by the contacts with the Visiting Researchers (VRs) that the consortium will invite (Obj. 2). This amounts to a minimum of 150 ECTS for a 3-year PhD program and 210 ECTS of a 4-year program.
- Practical training: Part of the training will be obtained by working on real cases provided by the partner organisations. This will take place during the PriMa Network Training Events and during the partner secondments. This will train the ESRs to handle real privacy protection problems. The secondments will contribute to the development of transferable skills such labour organisation, human resource management and cross-department communication which are relevant for the researcher's career perspective (Obj. 3). ECTS for this part are included in PriMa Training Events and Active Research.
- Attending local courses: Local courses at the host or secondment institutions, taught by experts within the PriMa consortium, will provide the ESRs with the basic general knowledge needed for their projects. Examples are taught modules on computer security, cryptography, machine learning, computer vision, statistics, and biometrics (Obj. 1). Each of the taught modules will be at a higher (Masters and above) level of content. Expressed in ECTS, local courses will contribute a minimum of 8 ECTS. The local courses to be undertaken by each ESR are defined in Table 3.1d.
- Attending PriMa Training events: PriMa Network Training events, including Workshops and Research Events (Table 1.2b) aim to provide the knowledge that is specific for becoming an expert in privacy protection. The PriMa Training Events will also provide training in complementary research skills, such as research management, ethics and IPR (see below) (Obj. 1). Expressed in ECTS, this amounts to 7 ECTS.

Transferable Skills Training: The primary goal of transferable skills training is to provide the skills that the ESRs will need during their professional and research careers (Obj. 1, 2 and 3). PriMa will provide comprehensive training in: 1) Management of research and development; 2) Communication skills; 3) Public engagement in science; 4) Science education; 5) Gender and ethics issues in science, Research Integrity, and Legal constraints; 6) Searching and applying for research funds; 7) Deployment of project results, standardisation and technology transfer; 8) Open access, Data management, and Data protection, including GDPR[75] and PSD 2[76]; 9) Career development skills; 10) Intellectual Property Rights; 11) Entrepreneurship and the creation of spin-off companies. The following mechanisms will support the ESRs with developing transferable skills:

- Attending local courses: Transferable skills as listed above will be provided by experts within in the PriMa consortium through local courses as they are offered in English by the PhD programmes of the graduate schools of the beneficiaries (e.g. Twente Graduate School, https://www.utwente.nl/en/education/post-graduate/tgs/prospective-candidates/phd/; UNIKENT's Unit for the Enhancement of Learning and Teaching and Graduate School https://www.kent.ac.uk/uelt/; UNIWUE's Graduate Schools, http://www.graduateschools.uni-wuerzburg.de/uwgs/general-information/). Examples of such courses, which are very similar for

[75] Ibid 23.
[76] Ibid 5351.

all beneficiaries, are: Personal Branding for PhD, Creative Thinking, Technical Writing & Editing, Time Management, Data Management. Expressed in ECTS, the local courses will contribute a minimum of 8 ECTS.

- Attending PriMa Training Events: The *PriMa Training Events*, including *PriMa Workshops* and *PriMa Research Events* (Cf. Table 1.2b) will provide training in transferable skills, such as research management, ethics and IPR. Expressed in ECTS, this amounts to 7 ECTS.

PriMa Training Mechanisms: The mechanisms that PriMa will put in place to structure and facilitate the training of the ESRs in research and transferable skills training are:

- **PriMa Training Events** (Table 1.2b) consisting of:
  - **PriMa Workshops.** A 3-day workshop will be organised yearly, where all ESRs will receive both transferable skills and research training. This training will be provided both by senior researchers from the beneficiaries and partner organisations, but also by invited speakers. ESRs will also provide an update on the progress of their individual research. The final workshop is the Dissemination Workshop, which is a public event, organised by the ESRs – thus providing dissemination training, where they will present their final results (Obj. 1, 2 and 3).
  - **PriMa Research Events.** Research Events are 3-day events, primarily focused on research training, where all ESRs will work together on topics created around challenges from one WP, thus extending the training beyond the ESR's own project. This joint work as well as the organisation of the Research Event, will be coordinated by the WP leader, assisted by the ESRs active in the associated WP, thus developing and putting into practice transferable skills regarding teamwork and project management. ESRs will also present their results and there will also be presentations by experts from within the network and invited speakers. The presentations at Research Events are open to a wider audience as experts and students in the fields will be invited to attend. In this way, the Events contribute to the dissemination of the results. Progress will be reviewed by a panel of experts, both internal and external to the network and from academia as well as industry. The review sessions are open to all ESRs, but not outside the network (Obj. 1 and 2).

  At each training event, a session will be dedicated to feedback from the ESRs on training and research organisation to improve PriMa and for the benefit of proposals for networks beyond PriMa. This feedback and the response to it will be laid down in deliverables D2.8 and D2.13.
- **Local courses:** Local courses at the host or secondment institutions will provide the ESRs with the research skills needed for their projects as well as transferable skills. Local courses will be complementary to the training offered at the training events (Obj. 1).
- **On-line training courses:** We recognise the role that on-line training resources have in a modern skills development environment. Each ESR will be exposed at a local level to these resources as directed by their supervisors (using materials that are relevant to their research) or at Network level (covering transferable skills subjects and technical aspects overarching the entire theme of PriMa). We shall leverage existing connections and material from external bodies such as EAB and the Biometrics Institute for these on-line courses.
- **Secondments:** All ESRs will undertake one 4-month secondment to an academic beneficiary and one to a partner organisation, as far as possible in different EU member states. The beneficiary secondments of paired projects are consecutive, such that the ESRs in the paired projects have the opportunity to work closely together over a period of 8 months. When possible, the beneficiary secondments are across multiple WPs, thus broadening the insight of the ESR in the topic of privacy protection. The partner secondments are chosen such that they fit closely to the ESRs project, giving the ESR the possibility to apply his/her knowledge in practice as well as to take challenges from industry to academia. Both types of secondments intend to improve the ESRs' research abilities as well as to broaden their perspective on the topic, achieving a more multidisciplinary viewpoint. Prior to the starting, the work of the ESR during of the secondment, including the local research and transferable skills training, will be defined in a discussion between the supervisors at the host and secondment institutions and the ESR. A summary of the secondments of each ESR in shown in Table 3.1d. (Obj. 1, 2 and 3)
- **Industrial Mentorship:** A unique aspect of PriMa's transferable skills training is the assignment of an *Industrial Mentor* to each ESR, who will guide the ESR in the development of transferable skills and in relation to career development. This will be a researcher from the organisation of the partner secondment. ESR and industrial mentor will meet during partner secondment and at the training events. (Obj. 1 and 3).

Table 1.2b Details of PriMa Training Events

Event	Name	Contents	ECTS	Lead	Month (est.)
TE1	Kick-off Workshop	*General:* Network introduction to all ESRs. Introduction of the participants and network paths. Practical information on network operation. Non-academic team building exercises;	0	UTW	11
		Research Training: State-of-the-art in biometrics and machine learning. Setting up of experiments including data collection and evaluating results.	0.5		
		Transferable Skills Training: a) How to organise ideas. b) Research integrity. c) Open Access & Data Management. d) Work planning.	1.5		
TE2	1st Research Event	*General:* Evaluation on the progress of the ESRs.	0	NTNU	17
		Research Training: Seminars from industry and academia. Privacy Analysis Study: A three-day event where ESRs work in teams on selected topics regarding the analysis of the privacy sensitivity of upcoming and established biometric modalities and on the analysis of privacy risks due to cloud storage and processing and activity on the internet. This study is related to the work in WP4 but will involve technical as well as legal aspects.	2		
TE3	2nd Workshop	*General:* Update on the progress of research projects. Industrial and academic State-of-the-Art update.	0	KU Leuven	23
		Research Training: Training on Legal and Ethical aspects of Privacy Preservation and Privacy Research.	0.5		
		Transferable Skills Training: a) Industrial Property Rights: Patents and Software Registry. b) Legal constraints for personal data: regulations and data protection including GDPR and PSD2. c) Gender & Ethics issues in science, including deontology. d) Public Engagement in science.	1.5		
TE4	2nd Research Event	*General:* Evaluation on the progress of the ESRs. This event will also be a mid-term dissemination event.	0	UAM	28
		Research Training: Invited seminars from industry and academia. Privacy Mitigation Study: A three-day event where ESRs work in teams on selected topics regarding the prevention of unwanted biometric recognition, the protection of biometric data, the use of privacy preserving technologies in identity management. This study is related to the work in WP5 but will involve technical as well as legal aspects.	2		
TE5	3rd Workshop	*General:* Update on the progress of research projects. Industrial and academic State-of-the-Art update. Initial discussions on future initiatives beyond PriMa.	0	UNIKENT	35
		Transferable Skills Training: Looking ahead: public and private sectors, the opportunities for developing the professional career: a) How to write a PhD Thesis. b) *Academic track:* Grant and project proposal submission, Science Education, Public Engagement in Science. c) *Business track:* Opportunity recognition, Business modelling, Technical and financial management, Commercial exploitation of IP.	2		
TE6	3rd Research Event	*General:* Evaluation of the progress of the ESRs. Further discussions on future initiatives beyond PriMa. Internal evaluation of PriMa's accomplishments. Presentation of the results achieved by each of the research projects already finished.	0	UNIWUE	41
		Research Training: Impact Assessment Study: A three-day event where ESRs work in teams on selected topics regarding the assessment of the impact of mitigating technologies such as developed in WP5 on the user's acceptance of such technologies. This study is related to the work in WP6 but will involve technical as well as legal aspects.	2		
DW	Dissemination Workshop	*General:* Public presentation of final project results with invited guest speakers.	0	UTW, ESRs	46
		Transferable Skills Training: To be organised in Brussels by the ESRs, thus providing training in organisational skills.	2		
Total ECTS Research Training through PriMa Events			7		
Total ECTS Transferable Skills Training PriMa Events			7		
Minimum ECTS Research Training through Local and On-line Courses			8		
Minimum ECTS Transferable Skills Training through Local Courses			8		
Minimum ECTS for PhD Program			150		

1.2.2 Role of non-academic sector in the training programme

Within PriMa, the private sector is represented by 7 partner organisations (50% of the consortium), consisting of private research organisations, industrial companies, SMEs, and a bank. The partner organisations either work on solutions for privacy protection or require privacy protection for their products. The first group creates the opportunity to collaborate on innovative solutions for privacy protection. The latter group offers the opportunity to analyse privacy threats and to define solutions. Collaborations with the private sector will steer the research towards solutions that are industrially and societally viable. Likewise, it will aid the translation of challenges that industry has to cope with related to privacy protection into inspiring academic research problems. Through partner secondments, industrial mentorships and involvement in training events, the partner organisations will contribute substantially and indispensably to the training of the ESRs. Interaction between academia and industry will assist in fulfilling the potential needs for privacy protection experts in the industrial sector in the near future. (Obj. 1, 2 and 3). Specifically, the role of the partner organisations in training will be:

- **To host partner secondments,** chosen to fit closely to the ESR's project, giving the ESR the possibility to apply his/her skills in practice as well as to take challenges from industry to academia. The secondment will also contribute to the transferable skills training of the ESR providing experience in, for instance, intra-company communication, project management and budgeting.
- **Active involvement in PriMa Training Events,** where partner organisations will present their activities on privacy protection, thus covering the technical and societal industrial contexts. They will also provide Technical Skills training with a focus on industrial aspects and industrial career planning.

- **Industrial Mentorship that** will guide each ESR throughout his project in the development of transferable skills and in relation to career development.
- **Active involvement in the management of the network** through the Supervisory Board (SB, Section 3.2).

1.3 Quality of the supervision

1.3.1 Qualifications and supervision experience of supervisors

To achieve successful completion of their training each ESR will have at least three supervisors, guaranteeing appropriate supervision during all stages of his/her research:

1. A principal scientist from the ESR's host institution will act as primary supervisor, whom the ESRs can refer to for the performance of their professional duties at all times during their training.
2. A principal scientist from the institution of the beneficiary secondment will act as co-supervisor, thus contributing to the inter-disciplinarity of the supervision and its continuity during beneficiary secondments.
3. A researcher from the organisation of the partner secondment will act as an industrial mentor. This will contribute to the inter-disciplinary character of the supervision and to its continuity during partner secondments.
4. Some beneficiaries will provide additional secondary supervisors, contributing to the continuity of supervision.

Each supervisor, primary or secondary, will guide the ESR in his specific field of expertise. The emphasis of the guidance by the academic supervisors will be more on research training, whereas the emphasis of the guidance by the industrial mentor will be more on transferable skills. The primary supervisor will be responsible for overseeing the complete training. All supervisors are experts in supervising research, have the time, knowledge, experience, expertise and commitment to be able to offer the ESR appropriate support and provide for the necessary progress and review procedures, as well as the necessary feedback mechanisms.

Face-to-face meetings with the primary supervisors will be on a weekly basis when the ESR is at the host institute. In these meetings progress and plans will be discussed and reviewed and the ESR will be provided with constructive feedback regarding his/her performance. When the ESR is on secondment, these progress meetings will be with the co-supervisor or with the industrial mentor and the primary supervisor and the ESR will have bi-weekly contact via teleconferences. Physical meetings of the ESR with the supervisor, co-supervisor and the industrial mentor will be scheduled twice per year at the Training Events. Primary supervisors will be present at the Training Events to obtain an external review of the progress of their supervised ESRs. These meetings will enable supervisors to identify opportunities for improving the training of their ESRs. Throughout the project the ESR will have contacts on an ad-hoc basis with the co-supervisor and industrial mentor through teleconferences. Before the ESRs will start their work, the three supervisors will prepare a training plan that will be laid down in the Career Development Plans.

All primary supervisors and co-supervisors have substantial expertise in guiding researchers towards a PhD degree. During partner secondments, the ESR will get additional support from his/her primary supervisor if needed. All beneficiaries adopt the European Charter for Researchers within their Rules and Protocols concerning the supervision of ESRs, in that the supervisor(s) assigned have sufficient expertise in supervising research, have the time, knowledge, experience and commitment to be able to offer the ESR appropriate support and provide necessary progress, review procedures and feedback mechanisms. Primary and co-supervisors and their ESRs are listed in Table 1.2c below. A description of the experience and the role of each beneficiary supervisor is given in Section 5.

Table 1.2c Assignment of supervisors

Name	Institution	ESR Primary supervisor	ESR Co-supervisor	Name	Institution	ESR Primary supervisor	ESR Co-supervisor
Prof. Dr. Raymond Veldhuis	UTW	3,9	6,11	Prof. Dr. Paul Pauli	UNIWUE	12	7
Prof. Dr. Farzin Deravi	UNIKENT	6	3	Prof. Dr. Marc Erich Latoschik	UNIWUE	13	5
Dr. Richard Guest	UNIKENT	2	1	Dr. Els Kindt	KU Leuven	5,14	13,10
Prof. Dr. Christoph Busch	NTNU	4	8	Dr. Ruben Vera-Rodriguez	UAM	1	2
Dr. Bian Yang	NTNU	10	14	Prof. Dr. Javier Ortega-Garcia	UAM	8	4
Dr. Bjarte M. Østvold	NRS	7,11	9,12				

1.4 Quality of the proposed interaction between the participating organisations

1.4.1 Contribution of all participating organisations to the research and training programme

All participants will participate in the research and training programmes, designed in WP2. All beneficiaries and partner organisations will be represented on the Supervisory Board and hence will participate in the evaluation of the implementation and the progress of the training programme and the research lines developed in WP4 –6.

The contribution and the workload of the beneficiaries is well-balanced, because: 1) Each beneficiary will supervise two ESR projects and host two secondments. 2) The responsibility for key activities, such as WP leadership and definition of material relating to training and dissemination, has been distributed evenly over the beneficiaries. UTW (as coordinator) has a higher load, because of the coordination and reporting. 3) Partner organisations will host two secondments (but not simultaneously to prevent overloading) and will contribute to the training events.

1.4.2 Synergies between participating organisations

Most of the beneficiaries in PriMa have known each other for several years by actively working together in projects, or by attending meetings and conferences, thus maximising the opportunities for a synergetic collaboration. Their specific expertise is listed in Table 1.4a in terms of PriMa's WPs. The numbers in this table refer to the ESR projects.

Table 1.4a Expertise of beneficiaries, numbers refer to ESR projects

WP	Topic	UAM	UNIKENT	UTW	NTNU	NRS	UNIWUE	KU Leuven
4	Analysis of Privacy Risks	1	2	3	4			5
5	Privacy Protection	8	6	9	10	7,11		
6	Impact Assessment of Privacy Protection						12,13	14

The beneficiaries represent specialists in privacy protection, biometrics, security, psychology, law and ethics, which are the necessary elements for successful research training in privacy protection. Each is an internationally renowned centre of excellence and can contribute to other ESR projects and training by bringing a wider perspective. The consortium is well-balanced in that there is a clear separation of main focus of expertise between beneficiaries but with sufficient overlap in the periphery to enable effective secondments and knowledge exchange, in particular in the paired projects. The partner organisations have been selected to support the individual ESR projects and training through partner secondments and training events. There is a natural synergy as they are all involved at the leading edge of development or usage of privacy protection and can contribute a distinct but complementary training component to the PriMa network. Figure 1.4.1 shows the beneficiaries and the themes of the paired ESR projects that exploit the synergy are given along the lines that connect them. The numbers correspond to the paired ESR projects that the synergy is exploited through by beneficiary secondments. The partner organisations are shown in yellow. The numbers along the lines that connect beneficiaries and partner organisations correspond to the ESRs that will do secondments at the partner organisations.

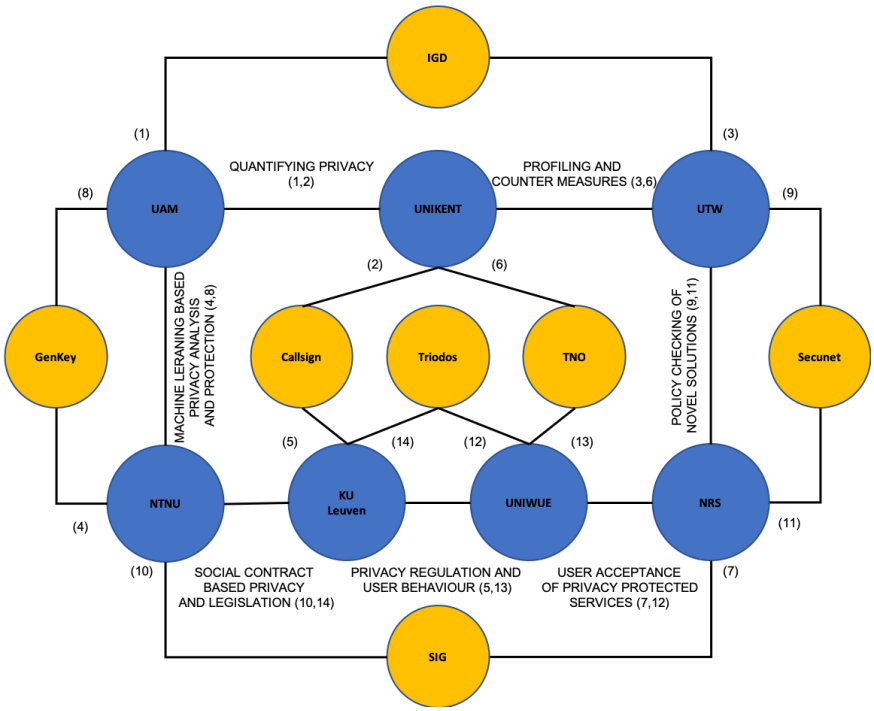

Figure 1.4.1 Synergy between beneficiaries (blue) and links to partner organisations (yellow). The numbers indicate the ESR projects. The joint expertise between paired projects is indicated as well.

1.4.3 Exposure of recruited researchers to different (research) environments, and the complementarity thereof

The ESRs will be exposed to different environments through secondments and training events. The beneficiary secondment will take place at the institute of the paired project. In most cases the pairing is chosen across WPs, such that the type of research is complementary, e.g. analysis versus mitigation, or mitigation versus impact (Table 1.2.a). In addition, each of the Research Events is also dedicated to a specific type of research (i.e. Analysis, Protection, Impact and Legal). The secondments at the partner organisations will bring the ESRs in contact with the typical aspects of industrial or applied research and will allow them to apply their results to non-academic sectors and to receive feedback in order to enhance their research. Within the training events, partner organisations will provide and reinforce transferable skills by using examples of current products, services and projects. They will provide a

direct link with areas such as banking and insurance requirements, governmental applications and health care services, as well as the needs of system integrators. Additional exposure to industrial sectors will be addressed by participating in dissemination activities with an industrial focus, such as visiting exhibitions and by requesting participation at industrial conferences. In such events, contact with major players in each of the above-mentioned sectors will be achieved, presenting the work of the researchers in order to attract attention and receive valuable feedback whenever possible. The European-wide nature of PriMa means that researchers are exposed to a wider culture and working environment, which will have clear benefits for a career in an international setting.

2. Impact

2.1 Enhancing the career perspectives and employability of researchers and contribution to their skills development

After their training the ESRs are able to contribute effectively to the solution of the ever-growing problem of privacy protection. With the skills acquired they are urgently needed in IT industry and IT consultancy companies, academia (e.g. the areas of Data Science, Business and Management, Law), and governmental organisations (Data Protection agencies, Ministries). They will have capabilities to handle high complexity problems related to privacy protection making use of rigorous signal processing, pattern analysis and artificial intelligence. The ESRs will be able to face real-world system conditions and operational challenges, bridging the gap between lab concepts and market solutions. Currently there is an increasing demand for privacy protection experts in the following categories:

- Working for end-users to determine the requirements for solutions to be deployed. (ESR1,2,3,4,5,10,12,13,14)
- Working for manufacturers and system integrators, to provide robust solutions fulfilling requirements defined by end-users. (ESR5,6,7,8,9,10,11,14)
- Qualified evaluators that, acting as independent third parties, are able to assess the accomplishment of those requirements. (ESR1,2,3,4,5,10,11,12,13,14)
- Industrial and academic researchers to continue with the improvement of IT solutions in existing open areas such as privacy preserving data aggregation, data sharing and mining, blockchain based data market places and finance applications (ESR1—14).
- Educators to train the next generation of scientists and engineers in the subject. (ESR1—14).
- Researchers with an entrepreneurial mindset and the capabilities to start spin-off companies to commercialise their results and create new business opportunities. See Section 2.3.2 on exploitation of results and intellectual property.

Exposure to different organisations, offered in multiple ways by PriMa, will empower the ERSs with an enriched professional network including prominent actors in the fields of privacy protection, and with extended knowledge sources. At the same time, their involvement in PriMa's outreach activities will make them true ambassadors of privacy protection, capable of effectively reaching out to different audiences. Finally, the gender equality policy adopted by PriMa stimulates female fellows to pursue a career in this field, both in academic and non-academic environments.

2.2 Contribution to structuring doctoral/early-stage research training at the European level and to strengthening European innovation capacity

PriMa aims to make a significant contribution to the structure of doctoral/ESR training at a European level in the following ways:

- Organisations from 6 different EU countries will interact. This will broaden the experience of the ESR but also stimulate the participants to organise the training jointly at a European level and from an EU perspective, explicitly adhering to the Salzburg II Recommendations[77] and EU's Principles for Innovative Doctoral Training[78].
- Of the host institutions, UTW, UNIKENT, NTNU, KU Leuven, and UAM have endorsed The European Charter & Code for Researchers Code[79], ensuring that ESRs can enjoy the same rights and obligations. UNIWUE has its own code of conduct[80] guaranteeing equivalent. ESRs hosted by NRS will graduate at NTNU, which endorses

[77] https://eua.eu/resources/publications/615:salzburg-ii-recommendations.html
[78] https://euraxess.ec.europa.eu/sites/default/files/policy_library/principles_for_innovative_doctoral_training.pdf
[79] European Commission 2005. European Charter for Researchers and a Code of Conduct for the Recruitment of Researchers. https://euraxess.ec.europa.eu/sites/default/files/am509774cee_en_e4.pdf
[80] University of Würzburg, 2000. Guidelines for safeguarding good scientific practice and procedures concerning scientific misconduct. https://www.uni-wuerzburg.de/en/information-for/university-employees/wissenschaftliche-infos/good-scientific-practice/

The European Charter & Code for Researchers Code.

- The training includes EU legislations and regulations on privacy such as the General Data Protection Regulation (GDPR)[81], and the Payment Services Directive (PSD 2)[82].
- Most ESRs will work in 3 EU countries: of their host, the beneficiary secondment, and the partner secondment.
- The Dissemination Workshop and the Research Events will be open, allowing a wider audience to benefit.
- We will disseminate PriMa's pedagogical best-practice through university, national, and international channels, highlighting the application of the structure to other thematic areas.
- PriMa's teaching material (slides, notes, videos) will be made publicly available through the PriMa website, subject to legal consent of the partner organisations involved.

The growing concerns about privacy are characteristic for the European society and market as has recently been identified by OECD[83], the UN Internet Governance Forum[84], and the EU[85]. Adopting a privacy-by-design approach will give the European IT industry a competitive advantage over competitors outside the EU. Therefore, we envisage that the ESR projects, with their direct integrations into novel industrial solutions, will enable lasting impact, and place PriMa and the EU at the leading edge of privacy protection innovation. PriMa's contribution to standardization will strengthen EU's innovation capacity. Finally, UTW as coordinator is member of the CESAER association[86], contributing to the realization of open knowledge societies, delivering significant scientific, economic, social and societal impact.

2.2.1 Contribution of the non-academic sector to the doctoral/research training

The contribution of the non-academic sector to the training programme is driven by an innovative secondments approach. Although industry has had an important role in doctoral training (for example in the UK's CASE award scheme), involvement is still scarce. Within PriMa we have a range of partner organisations each with an interest in leveraging cutting-edge academic research and to contributing to the development of talented researchers in the field. PriMa includes the integration of the non-academic sector within all areas of its activities. PriMa presents a novel framework applied to privacy research in that industry will play a key part in defining research pathways linked with transferable skills. We shall disseminate best practice of industry involvement within our network structure as defined in Section 2.3. In addition, we shall engage with industry to illustrate the benefits of supporting doctoral projects to further promote the growth of collaborations with industry as an integral part of doctoral training. To strengthen the competencies of ESRs required to be successful in industry, PriMa partner organisations commit to transfer practical knowledge with respect to the organisation and co-ordination of non-technical activities for successful implementation of the various innovative research activities. The 4-month secondment spent at a partner organisation will provide the ESR with very relevant industrial experience that will enhance the ESRs career perspectives.

2.3 Quality of the proposed measures to exploit and disseminate the results

All PriMa's communication, dissemination, and exploitation activities, including IPR and standardisation, are organised in WP3, led by NRS. PriMa has specific expertise in overseeing activities relating to dissemination (Spreeuwers, UTW, editorial roles), standardisation (Deravi, UNIKENT, leading EU player) and exploitation and IPR (Østvold, NRS, technology transfer). The consortium includes beneficiaries and partner organisations fully equipped with outreach resources that will help ESRs in adopting the appropriate means and language for their dissemination and communication activities. All members have their own, well-established communication and dissemination channels.

2.3.1 Dissemination of the research results

Our aim is to disseminate information concerning the expertise, research and integration activities of PriMa, as well as the new know-how that emerges from our research, to inform the public, influence policy-making and to encourage take-up by industry and other stakeholders, both in Europe and worldwide. It is our ambition that through our activities PriMa will become a global focus for expertise in data privacy and protection. A detailed Dissemination

[81] Ibid 23.
[82] Ibid 53.
[83] Ibid 1.
[84] Ibid 2.
[85] Ibid 3.
[86] http://www.cesaer.org/en/about/about-cesaer/.

Strategy will be developed within the project as part of WP3, however ESR supervisors, as senior researchers, take the lead in ensuring that research results are either exploited commercially or made accessible to the public (or both) whenever the opportunity arises in compliance with the Dissemination principles within the European Charter for Researchers[87]. *All of the principles described below shall be encapsulated and agreed between the Beneficiaries within our Dissemination Strategy*.

The work of PriMa will also directly respect the notion of 'Open Science' through the use of new platforms for sharing, collaborating and disseminating research data and outcomes to an EU and global audience through open access publications. We foresee four routes for dissemination, addressing different stakeholders and audiences:

Academic: We shall publish our results in high-quality peer-reviewed journals and conferences across our field. Journals where the partners have previously published high-quality papers in the sub-disciplines covered by PriMa include *IEEE Transactions in Human Machine Systems, Information Forensics and Security*, *IET Biometrics, Pattern Recognition*, *Computers in Human Behavior, Applied Ergonomics*, *Computer Law and Security Review, European Data Protection Law Review, Oxford International Data Privacy Law Journal,* and *Oxford International Journal of Law and Information Technology*, whilst major annual biometrics and privacy related conferences include *BTAS, ICB, FedCSIS,* and *IFIP Information Security & Privacy*. Given the public-funded nature of the proposed network we shall seek to publish through interdisciplinary open-access routes such as *PLOS ONE*. To fund these open-access publication activities, we shall draw upon individual beneficiaries institutional publishing funds where available.

Each of the ESR projects will produce a series of academic papers. Although it is difficult to predict exactly the quantity (and timing) of the production of these works, broadly we expect ESRs to produce a State-of-the-Art review in the first year of their study and at least two papers detailing results/experimental outcome in Years 2 and 3. We also anticipate that publications will arise which will be jointly authored by two or more of the participants (for example as outcomes of work at network events or through secondments). The summation of research conducted by each ESR will be described in a PhD thesis. Because some beneficiaries run 4-year PhD programmes, the final deliverable of an ESR after his or her 3-year appointment will either be the submission of PhD thesis or a final report (with the expectation that a thesis will follow later with the PhD programme). We fully expect that our parter organisations will be co-authors on academic outputs produced with their seconded ESRS (where non-commercially sensitive data permits).

Where jointly authored work is being submitted, all parties will be given a set period to comment and reflect on a manuscript prior to submission. Likewise, parter organisations will be given the power of veto over the publication of commercially sensitive technologies and results.

Industrial: The partner organizations will contribute to the dissemination of results within their own professional and consumer communities/networks. The work undertaken within PriMa has the potential to be directly commercialised through our partner organisations. This will be the primary route for industrial engagement, but where permissible, we shall engage with the wider stake-holder community through the distribution of an electronic newsletter (distributed twice a year) and at professional network events (such as the European Association for Biometrics) detailing major findings and events Our technology partners (GenKey, Security Networks, Callsign) are best placed to promote and disseminate the activities of PriMa through their client networks and trade shows. Our research organisation partners (IGD and TNO) will be able to build on the work of PriMa to inform and initiate other collaborative research activities within and beyond Europe. Our banking partner (Triodos) and consultancy partner (SIG) will be well placed to directly disseminate and utilise the results emerging from PriMa to their client base and the wider banking and related communities.

Public*:* Respecting the concept of Open Science, our aim is to improve: 1) the social awareness about the issues concerning privacy aspects of digitalisation through public engagement; 2) the impact of the PriMa's solutions; and 3) to create a deeper understanding of privacy by European citizens, through the creation of publicly available media and participating in public conferences and technological fairs. Our public engagement plans are detailed in Section 2.4.1, which also details the parter organisation involvement with these events.

Governmental and End-Users: Our results have the potential to directly impact governmental policy and industrial standards. We wish to reach out to European communities and explain the purpose and challenges of IT solutions, and how PriMa can support initiatives towards objective evaluation and mitigation of privacy challenges of biometric systems, and, importantly to shape future policy concerning these technologies. A major strength of the

[87] https://euraxess.ec.europa.eu/jobs/charter/european-charter

PriMa consortium is that we can leverage a range of existing liaisons including international standardisation, European and international stake-holder organisations (for example, EAB, the Biometrics Institute, IFIP) and provide input to a number of member-state governmental bodies through training activities, committee events/briefings and expert evidence. Several mechanisms will be used for general dissemination:

- On-line dissemination (through the PriMa website) and electronic newsletters. This information will also contain links to detailed scientific results and progress made.
- Workshops and Research Events, the Mid-Term Dissemination Event, and the Dissemination Workshop. When applicable, training material used at the training events will be made available through the PriMa website.
- Using social networks (such as Twitter) to raise the profile of the issues addressed within PriMa, publicise relevant articles from outside the Network and advertise Network outputs and events. Our aim is to provide reassurance and increase the social acceptance of the technology, not only to industry professionals, but also among citizens as end-users of the technology.

The Supervisory Board (SB) will be in overall control of dissemination and exploitation. This is especially important considering balance imposed by the potential sensitivity of the topics under consideration and the requirement for the academic participants to publish their work. WP3 will carry out the day-to-day management, strategy implementation and reporting of dissemination and exploitation. WP3 will also be responsible for managing the standardisation issues from the project work and for the design, development and delivery of the outreach activities. It is important to note that WP3 will be in charge of the coordination of the dissemination activities, but the specific dissemination will be carried out by the relevant WPs. Therefore, the dissemination of the research results will be handled directly by the research WPs (i.e. WP4-6).

2.3.2 Exploitation of results and intellectual property

WP3 will develop policies for the exploitation of results including standardisation, and monitor IPR constraints. The Supervisory Board will review the results every six months. PriMa's results are of primary interest to policy makers, manufacturers and end-users. It is, therefore, of primary importance that appropriate exploitation routes are defined in Task 3.5. For example, application of the results in biometrics template protection (Tasks 5.3,4) will raise the confidence of end-users in IT solutions and services. The work on evaluation will help manufacturers and clients to compare products and decide on solutions that fit the end-user's needs. Our exploitation objectives are:

1. To extend the existing roadmaps into a focused view of the evolution of IT solutions within Europe.
2. To exchange information and results among the researchers in PriMa and the wider community.
3. To facilitate the integration of a strong collaborative framework, to allow expert groups to effectively collaborate within the network on key topics to exploit results. Beneficiaries will bring their TTOs in contact with the ESRs to explore further exploitation of results.
4. To help ESRs with an entrepreneurial mindset to start spin-off companies to commercialise their results. Incubators present at the beneficiaries (e.g., http://www.kennispark.nl/?s=spin-off at UTW) will help the ESRs to realise this. If a beneficiary does not have an incubator, the ESR can obtain help from UTW.

Standardisation activities (Task 3.2) will be an effective route for dissemination, exploitation and societal change. Most participants in PriMa are active members of standardisation bodies such as ISO/IEC JTC1/SC17: Identification Cards, ISO/IEC JTC1/SC27: Security in Information Technology, ISO/IEC JTC1/SC37: Biometrics and CEN TC224: Identification Technologies. In addition, some of the beneficiaries of PriMa are currently named as the head of delegation of their National Bodies at international meetings/working groups. This involvement provides an effective method to enable multiple contributions to the standardisation world from the deliverables of PriMa, as well as paving the path for future exploitation of the results through technology transfer. We shall also draw upon participants' existing membership and key participation in trade associates such as the EAB, Biometrics Institute and IFIP to drive the dissemination of the wider community. We believe the standardisation and industrial integration of implementable technologies will lead to long-term impact for the results of PriMa.

Regarding IPR, Task 3.3 will define what will be considered as background knowledge that must be shared in order to maximise impact of the ESRs' work. All beneficiaries agree that foreground knowledge developed in network will be owned by the beneficiaries who produced it, but other beneficiaries will be granted access rights on a royalty-free basis for internal research activities. Any exceptions will be addressed in a Consortium Agreement according to the DESCA model[88]. Specific Partner Agreements regarding IPR will be made with the partner organisations.

[88] DESCA 2016. Horizon 2020 Consortium Agreement. http://www.desca-2020.eu/about-desca/

Consortium and Partner Agreements will contain procedures to deal with conflicts.

2.4 Quality of the proposed measures to communicate the activities to different target audiences

2.4.1 Communication and public engagement strategy

PriMa's results are directly applicable to technology that an ever-growing number of EU citizens use. Therefore, it is extremely important to explain how these results may be used to enhance privacy within their everyday lives. The ubiquity of the technology areas addressed in PriMa presents a huge opportunity for large-scale impact. Within this work all participants shall build upon previous expertise of communication and public engagement (such as local and national public communication lectures), adhering to the ethos outlined in the European Charter for Researchers in that we are ensuring that research activities are made known to society at large in such a way that they can be understood by non-specialists, thereby improving the public's understanding of science. The direct engagement with the public will help the ESRs to better understand its interest in science and technology, as well as its concerns. WP3 will produce as deliverable D3.2 a Dissemination and Communication Strategy, clarifying objectives, means, timeline and audiences for PriMa's diverse public engagement and outreach activities summarised in Table 2.4a.

Table 2.4a: Public Engagement Activities

Activity	Host	Key Audience	Expected Outcome and Measurement
Project launch news on websites of each of the participants' home pages	All beneficiaries	Industry, Government, Scholars	Awareness of project launch and objectives. Assessed by number of news story web-page 'hits' – anticipated impact: 10,000.
Development and update of PriMa website	NTNU	Industry, Government, Scholars, General Public	Launch of PriMa website containing information on project aims, objectives, events and consortium information. Updated with publications, results, news and developments. Assessed by number of webpage 'hits' – anticipated impact: 20,000
Press releases on news stories	All beneficiaries (Managed by institutional press offices)	Industry, Government, General Public	Awareness of news generated by the network. Assessed by take-up of press interest and follow-up by stakeholders – anticipated impact: 200 media outlets, commercial and public follow-up.
Public lectures, visits to high schools	All beneficiaries. Parter organisations will tailor releases to their customer-base.	General Public interested in science.	Communication of concepts and findings to a general audience. Assessed by attendance and feedback – anticipated impact: 500 members of the public
Press releases to scientific dissemination platforms	All beneficiaries	Industry, Scholars	Awareness of scientific news generated by PriMa. Assessed by take-up of press interest and follow-up by stakeholders – anticipated impact: 200 members of the scientific community.
Social networks (including http://www.esn-eu.org/home/index.html)	UTW	Industry, Government, Scholars, Public	Short communication on network outcomes – typically 3 a week. Assessed by number of 'reads' and follow-up by stakeholders within other events or direct communication.
Short YouTube videos introducing ESR projects to a wide audience	UTW	Public	Awareness of problems addressed by the network and general understanding of the solutions. Assessed by likes and comments.
Public scientific events (e.g., Open Days, Careers' Days, EU Researchers' Night)	All beneficiaries. Parter organisations will provide demonstrator equipment and engagement material.	Public	Public awareness of privacy-related issues. Assessed by number of visitors and follow-up by stakeholders – feedback – anticipated impact: 5000 members of the public, including children.

Importantly, as part of our dissemination and communication plan, we will hold two events that allow engagement with a wide range of stakeholders. The first is a mid-term dissemination event as part of TE4 in M28 (Section 1.2.1). Its aims are to present the results to interested parties outside the PriMa consortium. We shall draw upon our existing and substantial links with government, industry, academia and the public representatives as invitees to this event. The dissemination finale is the Dissemination Workshop in M46. This event, to be located in Brussels, will be open to the public, policy makers, industrial, governmental and research leaders, and academics and will present the results achieved by each of the ESRs, solicit exploitation routes and advice, review of the whole PriMa Network and produce a roadmap of activities beyond PriMa to feed into future EU initiatives and public understanding.

3. Quality and Efficiency of the Implementation

3.1 Coherence and effectiveness of the work plan

3.1.1 Fellow's individual projects

Table 3.1d Individual Research Projects

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR1	**UAM**	**Y**	**M07**	**36 Months**	**D4.1,3—7**
Project Title and Work Package(s): Quantifying Privacy with Application to Mobile User Interaction (WP4)					
Objectives: The scientific goal of this project is to develop theory and methodologies to quantify privacy in the context of data (traditional biometrics as well as touch and movement patterns, soft biometrics, and context information) acquired through the interaction of the user with mobile devices. A systematic study of the state of the art will be carried out. Multimodal datasets containing mobile user interaction data will be collected. New methods and metrics to better quantify privacy will					

be proposed and applied to the biometric data under consideration in continuous authentication schemes.

Expected results: 1) New multimodal datasets containing mobile user interaction data. 2) Study of the state of the art of privacy quantification in these scenarios. 3) Novel approaches and metrics for quantifying privacy under the considered scenarios.

Planned secondments: 1) A 4-month visit to ESR2 at UNIKENT (M13-16) where the ESRs will interact with the research team working on mobile device background sensors for continuous authentication and assess a range of privacy metrics. ESR1 and ESR2 have a number of common aims (albeit with different sensors) and hence this presents significant opportunities to interact. 2) A 4-month secondment with IGD (M26-29) wherein the ESR would trial a series of commercial behavioural solutions with the collected data. The expected outcome of this secondment is a commercially-focused set of results quantifying privacy in different combinations of behavioural biometrics.

Local courses: 2 courses from: Advanced signal processing, Machine learning, Biometrics, Computer human interaction, Developing interactive systems, Temporal information processing, Adaptive systems and user modelling, Bayesian methods, Big data, Data mining, Management of scientific and technological projects (all 6 ECTS MSc courses). For min. 8 ECTS from the transferable skills short courses: Property rights, Professional Effectiveness, Technical Writing & Editing, Effective presentations, Career counselling, English for lectures, Writing proposals, Communication skills, Systematically searching for information.

Fellow	Host institution	PhD enrolment	Start date	Duration	
ESR2	**UNIKENT**	**Y**	**M10**	**36 Months**	**D4.1,3—7**

Project Title and Work Package(s): Mobile Device Background Sensors: Authentication vs Privacy (WP4)

Objectives: This project will study the data-richness of background sensor data elements obtained from mobile devices in a continuous authentication scenario. We shall explore how 'personalised' data elements are, thereby providing an analysis as to which elements can enable accurate authentication, and by extension require the most privacy protection. In particular, we shall examine the sensitivity of combinations of data elements, the ability to infer one data element from another and how individuals and groups may be able to resist such challenges to their privacy. To facilitate this research, we shall both use existing datasets and collect background sensor data from devices across a representative population, conducted under an ethically approved protocol. Subsequently we shall analyse the data channels using temporal assessment techniques such as dynamic time warping to assess both intra- and inter-person variation. Our privacy analysis will use these variation data to assess both the quantity and type of samples needed to cause privacy concerns in the ability to be able to recognise a user. Finally, we shall explore a range of mitigation/hiding methods to protect these data from exposure, whilst enabling the possibility of a contribution to continuous authentication.

Expected results: 1) A dataset of mobile platform background sensor channel data. 2) A statistical methodology defined and applied to data channel data-richness, as well as performance assessment of single and multiple sources of authentication information. 3) Methods for mitigating data leakage to ensure privacy protection balanced against usable continuous authentication demands.

Planned secondments: 1) A 4-month visit to ESR 1 at UAM (M17-20) where the ESRs will interact with the research team working on mobile device interaction (e.g., swipe and signature) for continuous authentication and assess privacy metrics. ESR1 and ESR2 have a number of common aims (albeit with different sensors) and hence this presents significant opportunities to interact. 2). A 4-month secondment with Callsign (M30-34) wherein the ESR would trial a series of commercial behavioural solutions with the collected data. The expected outcome of this secondment is a commercially-focused set of results quantifying privacy in different combinations of behavioural biometrics.

Local courses: For min. 8 ECTS from: Image Analysis with Security Applications, Advanced Pattern Recognition, Computer Security, Advanced Biometrics, Pattern Recognition, Introduction to R, For min. 8 eq. ECTS from the transferable skills short courses: Research Techniques, Dissemination Techniques, Statistical Analysis, Approaching Employability, Personal Effectiveness, Ethics and Integrity.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR3	**UTW**	**Y**	**M10**	**36**	**D4.1,3—7**

Project Title and Work Package(s): Biometric profiling (WP4)

Objectives: The goal of this project is to analyse and mitigate the risk of biometric profiling on facial images and templates. It will investigate: 1) The risk of biometric profiling on facial images by inventorying attributes that can be inferred from these images. 2) The risk of biometric profiling on biometric templates of state-of-the-art facial recognition systems by inventorying attributes that can be inferred from templates. 3) The characteristics of the face and of the templates contribute to the inference of the attributes found under 1) and 2). Recommendations for the storage of facial images and the generation of biometric templates in order to reduce the risk of profiling will be provided.

Expected results: 1) Inventory of the risks of biometric profiling on facial images. 2) Inventory of the risks of biometric profiling on biometric templates extracted from facial images. 3) Study of characteristic of the face that are vulnerable to profiling. 4) Recommendations for the storage of facial images and the generation of biometric templates in order to reduce the risk of profiling.

Planned secondments: 1) A 4-month visit to IGD (M17-20) wherein the ESR would work study profiling on biometric templates other than face. The expected outcome of this secondment is a set of results focussing on the privacy sensitivity of voice templates. 2) A 4-month secondment with ESR6 at UNIKENT (M30-34) where the ESRs will study the effect of counter measures on profiling. ESR3 and ESR6 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding of how profiling can be prevented by Biometric Identity Hiding, Obfuscation and De-identification.

Local courses: For min. 8 ECTS from: Introduction to Biometrics, Basic Machine Learning, Theory and Practice of Deep Learning (all 5 ECTS MSc courses). For min. 8 ECTS from the transferable skills short courses: Professional Effectiveness, Technical Writing & Editing, Academic presentations, Career counselling, Career Orientation and Application, Creative thinking, English for lectures, How to write an individual research proposal, Interview skills in English, Perfecting your Publication, Presentation skills, Systematically searching for information, Workshop Personal Branding.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR4	**NTNU**	**Y**	**M07**	**36**	**D4.1,3—7**

Project Title and Work Package(s): Modelling Private Identity Management Behaviours by Digital Footprints (WP4)

Objectives: The goal of this project is 1) to quantify the relations between digital footprints and identity attributes, 2) to model these by statistical and machine learning methods, and 3) to study the dynamics of human behaviours in identity management under various scenarios before and after receiving privacy and security awareness training.

Expected results: 1) Quantitative models of the relations between digital footprints and identity attributes. 2) Models of the dynamics of human behaviours in identity management under various scenarios before and after receiving privacy and security awareness training.

Planned secondments: 1) A 4-month visit to ESR8 at UAM (M13-16) where the ESRs will study the robustness of privacy protection developed at UAM to machine-learning based attacks on private data devised by NTNU. ESR4 and ESR8 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding the robustness of privacy protection to machine-learning based attacks. 2) A 4-month secondment with GenKey (M26-29) where the ESR will interact with the research team working on template protection. The expected results are an understanding of the sensitivity of template protection to machine-learning based attacks.

Local courses: For min. 8 ECTS from: Biometrics, Behavioural Biometrics, Foundations of Information Security, Modern Cryptology, Selected Topics for Cryptology, Wireless Communication Security, Real-time AI for Robotics and Simulated Environments, Computational Forensics, Computational Intelligence (all 5 ECTS MSc courses). For min. 8 ECTS from the transferable skills short courses: Critical Thinking, Ethics and Legal Aspects of Scientific Research, Quality in Academic Research, and Scientific Communication. In addition, the ESR attend national COINS IT security workshops and summer and winter schools https://coinsrs.no/.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR5	**KU Leuven**	**Y**	**M10**	**36**	**D4.1,3—7**

Project Title and Work Package(s): Privacy and biometrics in health and activity tracking (WP4)

Objectives: The objective of this project is to evaluate the ability of some of the data protection concepts to manage the risks posed by the sensor-rich health and activity tracking devices that collect a wide range of (health-related) personal data from their users. These data are considered valuable assets by many companies which often rely on anonymization as a safe haven from the stringent data processing rules in the EU. The ESR will assess the legal viability of the existing privacy preserving measures and techniques against the background of growing computing power and the associated concerns of data linking and matching. The project will explore the possible legal avenues to mandate protection of these data if true anonymization would not be achievable in the near future. Furthermore, it will assess the legal implications of making inferences of a person's health based on collected behavioural biometric data by these devices. It will also study the durability of the finality and the purpose limitation principles given the potential of storing these data in public or hybrid cloud environments, use in remote clinical trials and use by third party applications leading to blending of both the processing purposes and the roles of the involved parties. The ESR will consider the relevance of the distinction between controllers and processors in a situation where multiple (international) data transfers take place between different parties in different jurisdictions.

Expected results: 1) Analysis and discussion on re-assessing the role of some of the fundamental privacy and data protection concepts. 2) Essential knowledge about the interpretation of the existing legal regime in the context of 'connected' tracking devices collecting behavioural biometric data and data concerning health. 3) Policy guidelines and recommendations for legislative improvements.

Planned secondments: 1) A 4-month visit to ESR13 at UNIWUE (M17-20) where the ESRs will study effects of privacy regulations on user behaviour in communication. ESR5 and ESR13 have a number of complementary aims and hence will interact concerning methodologies and analysis techniques. The expected results are an understanding of the effects of privacy regulations on behaviour in communication. 2) A 4-month secondment with Callsign (M30-34) where the ESR will study the interaction between engineering possibilities, fundamental rights and regulations. The expected outcomes are an improved understanding of the social and technological aspects of 'connected devices' and their legal and ethical implications.

Local courses: the courses provided as part of the LLM programme "IP and ICT law" of the KUL (campus Brussels) are accessible (https://onderwijsaanbod.kuleuven.be//opleidingen/e/SC_51863537.htm#bl=05), such as the courses of European Privacy and Data Protection law and European Electronic Business Law. Besides, the master programme "cybersecurity" taught at the CyberSecurity Akademie in Den Hague (https://www.csacademy.nl/en/), which provides interdisciplinary (including legal) perspectives on cybersecurity, is also accessible.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR6	**UNIKENT**	**Y**	**M07**	**36**	**D5.1,3—7**

Project Title and Work Package(s): Biometric Identity Hiding, Obfuscation and De-identification (WP 5)

Objectives: This project will investigate emerging and future approaches to sensor-level identity hiding. Examples of identity hiding include wearing a hat or using makeup to render facial detection and recognition problematic. Alternatively, direct interference with the sensor involves techniques such as projecting noise signals to directly interfere with the biometric sub-system. What is i) possible now, and also in the future, and ii) how the performance of such approaches can be evaluated, will be topics for research in this project across a range of modalities including face/iris, gate and voice. Hybrid approaches will also be investigated, where the user and the system cooperate in privacy preservation. In such hybrid systems, users may explicitly indicate the wish for identity hiding, obfuscation and de-identification to biometric and storage systems separately which in turn invoke the necessary processes to ensure compliance with privacy protection policies in force at the time of capture and storage. Understanding the links with psychological aspects of identity hiding and legal aspects of compliance of devices and systems to identity protection protocols are essential to the successful evaluation and deployment of any such technologies.

Expected results: 1) Methods for identity protection at presentation/sensor level for a range of modalities. 2) Collaborative techniques and protocols for identity preservation. 3) Metrics and methodologies for assessing the effectiveness of identity protection technologies.

Planned secondments: 1) A 4-month visit to TNO (M13-16) where the ESR will interact with the research team working with leading edge surveillance technologies. The expected results are an understanding of how identity hiding techniques impact the performance of surveillance systems. 2) A 4-month secondment with ESR3 at UTW (M26-29) where the ESRs will study the interaction between Biometric Identity Hiding, Obfuscation and De-identification and Biometric Profiling. ESR3 and ESR6 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding of how profiling can be prevented by Biometric Identity Hiding, Obfuscation and De-identification.

Local courses: Cf. ESR2.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR7	**NRS**	**Y**	**M07**	**36**	**D5.1,3—7**

Project Title and Work Package(s): Identity provisioning in the cloud: Privacy, security, and user experience when authenticating to services (WP5)

Objectives: The objective of the project is to describe how privacy, security and user experience are affected by design choices when building services that use cloud-based identities. Such choices include what personal data to collect and how and where to process the data and store it. Identity providers want to know our entire digital milieu to better identify us and to let us authenticate passively using our data, while users have privacy concerns. Project topics include formal modelling, secure authentication, security of cloud-based services, data analysis and its effect on privacy, and the relation between privacy, user experience and security. The scientific goal is to identify the core the principles of such identity provisioning, enabling a sound method for designing systems involving provisioning.

Expected results: 1) Formal model of data-driven authentication including users, services, and cloud-based identity providers. 2) Designs of data-driven identity provisioning, including how to distribute or segregate personal data, explaining how privacy, simplicity of use, and trust relations are affected. Cloud-based identities are seeing rapid increase in usage, which should make the fellow attractive in the job market.

Planned secondments: 1) A 4-month visit to SIG (M13-16) where the ESRs will apply their methods in real applications developed in SIG projects. The expected outcomes are that the ESR has acquired in-depth insight in real-life applications of privacy protection in the cloud and makes a contribution to a SIG project. 2) A 4-month secondment with ESR12 at UNIWUE (M26-29) where the ESRs will study the user acceptance of identity management in the cloud. ESR7 and ESR12 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding user acceptance of identity management in the cloud and design rules for such identity provisioning.

Local courses: being a research institute, NRS cannot offer courses, but local training will be provided at NTNU. Cf. ESR4.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR8	**UAM**	**Y**	**M10**	**36 Months**	**D5.1,3—7**

Project Title and Work Package(s): Privacy Protection in Multimodal Biometrics with Application to e-Learning and e-Banking (WP 5)

Objectives: This project will focus on state-of-the-art privacy protection techniques for multimodal biometric systems for two case studies of great interest for biometrics: e-Learning and e-Banking. The main scientific goals will be: 1) to analyse the main challenges and requirements of biometric template protection, both for security and privacy, in single and multi-modal biometric systems; 2) to evaluate several state of the art approaches, the information stored, the recognition performance, the potential advantages and limitations; 3) to review existing and propose novel metrics to measure the levels of noninvertibility, revocability and unlinkability of biometric templates for multimodal systems.

Expected results: 1) Multimodal datasets for e-Learning and e-Banking applications. 2) Methods for privacy protection in multimodal scenarios. 3) Metrics to measure the levels of noninvertibility, revocability, and unlinkability for multimodal biometrics.

Planned secondments: A 4-month visit to ESR4 at NTNU (M17-20) where the ESRs will study the robustness of privacy protection developed at UAM to machine learning-based attacks on private data devised by NTNU. ESR4 and ESR8 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding the robustness of privacy protection to machine-learning based attacks. 2) A 4-month secondment with GenKey (M30-34) where the ESR will interact with the research team working on protection of biometric templates. The expected outcome of this secondment is that the ESR has acquired in-depth insight in the application of privacy protection in real-life applications.

Local courses: Cf. ESR1

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR9	**UTW**	**Y**	**M07**	**36**	**D5.1,3—7**

Project Title and Work Package(s): Integration of biometric recognition and homomorphic encryption (WP5)

Objectives: Recent research has shown that a novel approach that integrates an optimal likelihood-ratio-based classifier for statistically independent features in a homomorphic encryption scheme results in a very fast implementation of biometric recognition under encryption with near optimal recognition performance. The approach works in a 2-party scheme where a client contains the biometric sensor and the templates are stored on a server. The scheme is secure in an honest-but-curious setting. The goal of this project is to develop this promising approach further. In particular, it will investigate: 1) The pre-processing and conditioning of biometric features of state-of-the-art biometric recognition systems so that they can work with a homomorphically encrypted likelihood-ratio-based (HELR) classifier for independent features. 2) Extension of the approach to other multi-party schemes and relaxation of the honest-but-curious requirement.

Expected results: 1) Implementations of HELR classifiers for face and fingerprint biometrics. 2) Multi-party schemes for encrypted biometric recognition with provisions for malicious parties.

Planned secondments: 1) A 4-month visit to ESR11 at NRS (M13-16) where the ESRs will work on the secure design of the software for the multi-party protocols for homomorphic encryption. ESR9 and ESR11have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected result is a secure software implementation of the protocols. 2) A 4-month secondment with Secunet (M27-29) where the ESR will apply his methods in real applications developed in Secunet projects. The expected outcomes are that the ESR has acquired in-depth insight in real-life applications of biometric recognition under homomorphic encryption as well as a contribution to a Secunet project.

Local courses: Cf. ESR3.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR10	**NTNU**	**Y**	**M10**	**36**	**D5.1,3—7**

Project Title and Work Package(s): Multi-party social contracts and privacy mechanisms (WP5)

Objectives: This project will investigate and model the interaction between technology innovation and legislation, measure the mutual impact, and explore the possibility to innovate the future privacy legislation procedures and methods by a technology-driven approach such as smart-contract-based social contract. It will focus on the questions: (1) Is it viable to model privacy by social contract in harmony with existing law and future legislation process and how to do this? (2) How to technologically enable the social contract concept in a secure and privacy-preserving way, e.g. to enhance distributed ledger technologies (DLT) and smart contract? (3) Will such social contract-based privacy personalisation models cause ethical and societal challenges (e.g., social inequality) and how to mitigate these risks?

Expected results: 1) Metrics for the performance of social contract. 2) Report on the status and feasibility of emerging technologies' impact on privacy legislation. 3) Recommendation of innovative social contracts for a better balance between security and privacy.

Planned secondments: 1) A 4-month visit to SIG (M17-20) where the ESR will study how the legislation process can be better designed. The expected outcomes are the better understanding of the impact and feasibility of new technologies on privacy legislations. 2) A 4-month secondment with ESR14 at KU Leuven (M30-34) where the ESRs will study the impact of supporting technology on the legislation process. ESR10 and ESR14 have a number of similar aims and hence this secondment presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding of the social contract concept and its technological implementations in the context of privacy protection.

Local courses: Cf. ESR4.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR11	**NRS**	**Y**	**M10**	**36**	**D5.1,3—7**

Project Title and Work Package(s): Detecting privacy problems in software (WP5)

Objectives: The objective of the project is to build tools that help software development organisations write software that complies with the new General Data Protection Regulation (GDRP) of the EU. The work will build on previous work on formal specification and on existing tools for property checking and analysis of software and protocols. The project shall extend and adapt these techniques to discover defects and design flaws related to personal data and privacy policies, including the treatment of biometric information in distributed systems. Key sources of inspiration is work on finding security defects in software and analysing cryptographic protocols and work on privacy by design. Project topics include privacy engineering and its relevance for software development, formal specification, and static analysis. The scientific goal of the project is to give an operational definition of the term "privacy defect" and thus enable its semi-automatic detection in software. Compliance with the GDPR is a key current concern for software enterprises, and thus the knowledge acquired by the fellow has high industrial relevance.

Expected results: 1) Precise definition of privacy defect and privacy design flaw, drawing on GDPR. 2) Specification language for privacy and policies connecting domain knowledge to the code. 3) Static analysis for checking code against specifications and its implementation as a prototype tool, e.g. a plugin to an existing integrated development environment.

Planned secondments: 1) A 4-month visit to ESR9 at UTW (M17-20) where the ESRs will work on the secure design of the software for the multi-party protocols for homomorphic encryption. ESR9 and ESR11 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected result is a secure software implementation of the protocols. 2) A 4-month secondment with Secunet (M30-34) ESR will apply his methods in commercial applications developed in Secunet projects. The expected outcomes are that the ESR acquires in-depth insight in real-life detection of privacy problem in software as well as a contribution to a Secunet project.

Local courses: being a research institute, NRS cannot offer courses, but local training will be provided at NTNU. Cf. ESR4.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR12	**UNIWUE**	**Y**	**M10**	**36**	**D6.1,3—7**

Project Title and Work Package(s): Acceptance and usage of privacy protection solutions (WP6)

Objectives: This project will examine the acceptance, usage and usability of various data protection solutions in daily life and under typical cognitive, social, and emotional states (e.g., stressful office, relaxed home, public meeting, private meeting), which will be induced by virtual reality. The user will be immersed in typical virtual situations and will be confronted with privacy protection or surveillance equipment. The behaviour as well as cognitive and emotional responses will be registered and analysed in order to allow conclusions about acceptance, usage and/or usability and possibilities to modify behaviour, e.g. on the basis of verbal or virtual instructions.

Expected results: 1) Data on the actual usage of and knowledge about existing privacy protection tools. 2) Assessment of the expectations about ideal data protection tools. 3) Knowledge on usage behaviour of different privacy protection tools under ecological valid conditions. 4) Conclusions how usage and acceptance of privacy protection tools in daily life can be improved.

Planned secondments: 1) A 4-month visit to Triodos (M17-20) where the ESR will study acceptance, usage and usability of various data protection solutions applied to e-banking. The expected outcomes are that the ESR has acquired in-depth insight into design aspects of privacy protection for e-banking. 2) A 4-month secondment with ESR7 at NRS (M30-33) where the ESRs will study the user acceptance of identity management in the cloud. ESR7 and ESR12 have a number of complementary aims and hence this presents significant opportunities to interact concerning methodologies and analysis techniques. The expected results are an understanding of user acceptance of identity management in the cloud and design rules for such identity provisioning.

Local courses: For min. 8 ECTS out of: Psychological methods; machine learning; multimodal interfaces; real-time interactive systems; theories of human-computer-interaction; methods of data analyses; (all 5 ECTS MSc courses). For min. 8 ECTS from the transferable skills short courses: poster presentation; good scientific practice; cover letter and CV; job interview; oral presentation; self-, time – and team-management; presentation skills for teaching; writing skills; presenting research in the sciences; English for business; intercultural competence

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR13	**UNIWUE**	**Y**	**M07**	**36**	**D6.1,3—7**

Project Title and Work Package(s): Privacy protection effects on social communication (WP6)

Objectives: Technology changes social communication in a way that direct personal contact decreases while technology-mediated communication increases. Thus, a user can create an optional picture of himself and even an avatar for communication. This, on the one hand, may help to protect privacy, but on the other hand,

may lead to anonymity that may dismantle social rules and restrictions. This project will examine how changing communication from surveillance to privacy and to anonymity will affect communication behaviour. The goal therefore is to determine if and how anonymity and privacy protection correlate with violation of social rules and how unwanted effects may be prevented.

Expected results: 1) Data on the frequency and the reasons for using anonymous identities in technology-mediated social communications. 2) Insight on how modified personality characteristics affect social communication. 3) Conclusions on how anonymity and privacy protection affect different kind if social communications. 4) Knowledge on the interplay between privacy protection and social behaviour.

Planned secondments: 1) A 4-month visit to ESR5 at KU Leuven (M13-M16) where the ESRs will study the effect of privacy regulations in health and activity tracking on user behaviour. ESR5 and ESR13 have a number of complementary aims and hence will interact concerning methodologies and analysis techniques. The expected results are an understanding of the effects of privacy protection on behaviour and health monitoring the legal context of privacy protection and communication. 2) A 4-month secondment with TNO (M26-29) where the ESR will study privacy protection effects on social communication application of TNO. The expected outcomes are insights in how anonymity and privacy protection correlate with violation of social rules and how unwanted effects may be prevented in a real application.

Local courses: Cf. ESR12.

Fellow	Host institution	PhD enrolment	Start date	Duration	Deliverables
ESR14	KU Leuven	Y	M07	36	D6.1,3—7

Project Title and Work Package(s) to which it is related: Legal digital identity: reconciling blockchains, biometrics and privacy (WP7)

Objectives: This project will study the role of blockchain-based systems as enablers of the creation of a legal digital identity for all individuals. The ESR will explore the legal feasibility of implementing an initial identity record on a blockchain upon individual's birth with information of relevant life events being added later in time. The project will examine the legal requirements for authentication of the owner of a particular record on the blockchain and the feasibility of a system based on dynamic biometrics. Particularly, it will consider whether a system could be based on two or more behavioural biometrics by connecting, for example, heart rate, movement, and location by means of smart devices such as a smartphone, body monitor and a smart watch. The researcher will look into the challenges of combining blockchain with biometrics as a way of providing more user control. The project will evaluate the fitness of the new General Data Protection Regulation for the distributed peer-to-peer architecture of the blockchain which involves multiple (personal) data transfers, making it extremely difficult to determine the 'classical duo' of controller(s) and processor(s). It will also consider the risks of irreversibility and transparency created by blockchains for the exercising of individuals' rights to rectification, erasure and restriction of the processing of their personal data. The project will assess from a legal perspective the 'dual' role of blockchains as reinforcers of biometrics' inherent weaknesses (e.g., compromised biometrics in an irrevocable and immutable blockchain) but also as enablers of stronger protection against interference by malicious third parties (e.g., cryptographically stored biometric data across multiple computers). This research will provide the foundation for a solution that holds account of the sensitivity of biometric data, provides sufficient safeguards to the right to privacy and benefits from the combination of blockchains and biometrics.

Expected results: 1) A legally sound theory and solution to the problem of legal identity by considering the pros and cons of identities based on the combined use of blockchain technologies and biometrics. 2) A draft legislative framework that takes into account the benefits and costs of such potentially global identity solutions from a legal point of view. 3) Recommendations for legislative improvements and guidelines for developers of such systems.

Planned secondments: 1) A 4-month visit to Triodos (M13-16) where the ESR will look into legal aspects regarding privacy-protected identity management in the context of e-banking. The expected outcomes are improved knowledge and awareness of the existing and future ID management solutions that will contribute to the development of a practicable legal solution. 2) A 4-month secondment with ESR10 at NTNU (M26-29) where the ESRs will study the impact of new technologies, such as the blockchain, on privacy and data protection law. The ESRs will look into innovative approaches to the legislative process that could provide valuable input for the development of a viable legal digital identity legislative framework within the project.

Local courses: Cf. ESR5.

3.2 Appropriateness of the management structures and procedures

3.2.1 Network organisation and management structure

PriMa's management structure, built on a division of the network tasks over 6 WPs, is shown in Figure 3.2.1. PriMa has 3 managerial WPs (WP1—3) and 3 research WPs (WP4—6). Central in the structure are the Network Coordinator (NC) and the Supervisory Board (SB), whose roles are discussed below. The work in the WPs is subdivided into tasks, managed by task leaders. Senior researchers of the beneficiaries will be appointed as WP and task leaders. The WPs with their lead beneficiaries and tasks are detailed in Table 3.1a. The WP leaders are responsible for the timely submission of deliverables (Table 3.1b) but can delegate the responsibility for the production of these deliverables to the task leaders. The communication within PriMa is organised in a structure of meetings. Table 3.2 shows the composition, format and frequency of these meetings. Formal regulations and responsibilities will be laid down in 1) the Description of Work that this document will become, 2) a Consortium Agreement between beneficiaries, 3) Bilateral Beneficiary-Parter organisation Agreements covering IPR and non-disclosure, and 4) Career Development Plans for the ESRs.

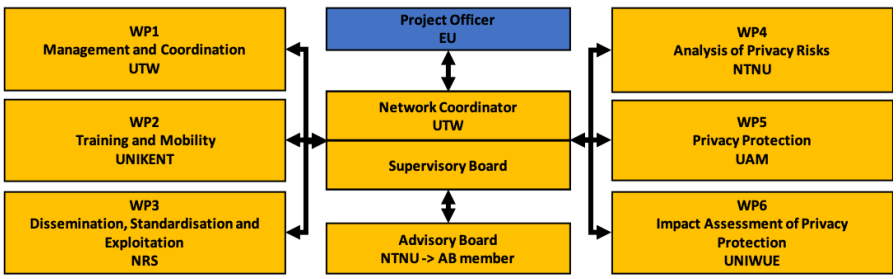

Figure 3.2.1 PriMa Management structure.

The Network Coordinator (Prof. Raymond Veldhuis, UTW) is responsible for the coordination of PriMa, which task is organised in WP1. He will be assisted by a part-time project administrator who will be appointed for this task. The NC will be the contact point between PriMa and the EC Project Officer (PO). Communication between NC and PO is foreseen to be primarily electronic, though the PO will be invited to all Supervisory Board meetings. If requested by the PO, the NC will attend a physical meeting. The NC will chair the SB (Section 3.2.4). The NC will also establish the communication with all beneficiaries and partner organisations. In order to keep the communication

active without overloading beneficiaries and partner organisations, the NC will establish monthly teleconferences with WP leaders, primary supervisors and ESRs. Any reserved business (for example, confidential information about an ESR's progress) will take place without the ESRs. A project manager will be appointed at UTW on a part-time basis to assist the NC with administrative duties.

The governance of PriMa will be handled by the SB (Section 3.2.4). All 6 WP leaders report to the SB. In addition to 6-monthly SB meetings, a set of whole-consortium meetings with the SB will take place in order to coordinate the activities of PriMa. A launch meeting is scheduled for M01, to be attended by all beneficiaries and the PO, followed by a Kick-Off Meeting (M10), which will join all beneficiaries, partner organisations and the ESRs, in order to provide information about PriMa structure and events, the training program, all management procedures and the dissemination and exploitation plan. Additionally, the End-of-Project meeting will serve for the review of the project by the PO and external stakeholders.

Financial Management is in WP1. The NC's institution (UTW) will be in charge of receiving payments from the EC and will proceed with the distribution of the advance payment at the beginning of the network. Each beneficiary will be responsible for its expenses and distribution of the assigned budget. Further payments will only be transferred from UTW to a beneficiary after the beneficiary fulfils all the financial conditions of this call. UTW will take €60,000 extra from the project funds reserved for Management to finance a part-time administrator. Agreement on the finances within the running of the ETN will be laid down in the Consortium Agreement. PriMa will benefit of the extensive experience that UTW has with Marie Curie and other EU research projects. Any financial issues requiring investigation will be resolved by SB with input from the PO if necessary. Beneficiaries that run a 4-year PhD program will finance the 4th year of their ESRs from means outside the project budget.

Training Management is handled by WP2, who will define, supervise and manage all training activities. As stated, training will be provided in specific and general research topics and also in transferable skills. Within the tasks of WP2, all training events will be detailed, planned and organised. WP2 will also coordinate the development of Career Development Plans for all ESRs and monitor their progress in association with their ESR supervisors.

Dissemination Management, including dissemination, standardisation, and exploitation of results, as well as IPR and Data Management is the responsibility of WP3.

Research Management: Research management will be hosted at WP level. Each research WP leader (WP4—6) will be responsible for overseeing, monitoring and directing where necessary the WP's research activities and will report at the SB meeting. Each ESR project is organised as a task in a research WP and primary supervisors at the host institutions will act as task leaders, being responsible for the day-to-day management of the ESRs.

Management of Conflict Resolution and Misconduct: Any required conflict resolution and scientific misconduct will be investigated and resolved initially at a WP level. The WP leader will investigate the issue with direct input from the ESR(s) and the academic supervisor(s). This will be conducted with collaboration of the ESR's host institution with reference to their rules and regulations governing academic discipline where appropriate. In the case that the WP leader is also the academic supervisor of the ESR involved, then the NC will lead an enquiry. Upon completion of the enquiry, the NC will make recommendations to the SB, who will decide on a resolution. It is anticipated that most conflict/misconduct issues can be dealt with between the ESR and the supervisor. However, if a repeated offence is conducted, or if the offence is deemed serious, procedures (as described above) will be instigated.

Table 3.2: PriMa Groups and Committees

Meeting Name	Chair	Format	Participants	Frequency
NC - PO Meeting	PO	Face-to-Face/ Electronic	NC, PO	As required
Monthly Telcos	NC	Electronic	ESR primary supervisors, ESRs, WP leaders.	Monthly
SB	NC	Face-to-Face (Electronic if needed)	SB, PO invited.	6 Months
Advisory Board	NTNU	Face-to-Face	External Advisors, WP Lead	Yearly
ESR Meetings	ESR Supervisor	Face-to-Face/ Electronic	ESR supervisor and ESR. Partner organisations when required.	Weekly

3.2.2 Supervisory board

The SB will be the centre of the management of PriMa. Chaired by the NC, it will comprise one representative (usually the lead researcher) from each beneficiary and partner organisation and an elected ESR representative. The SB will work as a democratic body where decisions will be presented and resolved. Each beneficiary will have a single vote, while partner organisations and the ESR representative will have an advisory function only. Decisions shall be taken by a majority of two-thirds (2/3) of the votes cast. . As the main management body, the SB will:

- Monitor progress by reviewing the work done in: **WP1**: Management and Coordination. This includes overseeing the recruitment of all ESRs and monitoring and assessing the compliance with all ethical and legal directives.

WP2: Training and Mobility. This includes overseeing the training of all ESRs. **WP3**: Dissemination, Standardisation, Exploitation, IPR, and Data Management. **WP4—6**: Research. In all cases the WP leader will report to the SB. Indicators for the evaluation of progress, e.g. rate of recruitment, research progress, acquired research and transferable skills of each ESR, and production of deliverables, will be produced as deliverable D1.2 of WP1.

- Develop and instigate the implementation of contingency actions in the WPs needed when unplanned deviations from the work plan are detected (e.g., re-scheduling some training events or re-allocation of researchers).
- Instigate the implementation of mitigations in the WPs for risks that occur (Cf. Table 3.2a).
- Take decisions on conflict and misconduct issues.

The SB will physically meet every six months at the Training Events. The PO will be invited to these meetings. Although recommended that each participant will be represented by the lead researcher, participants have the right to nominate another faculty member/senior research manager to represent them. The SB meeting will require at least a representative of each beneficiary and the ESR representative. An extraordinary meeting of the SB via teleconference can be arranged at any time if consensual decision is required. Scheduling of such meetings will be made well in advance as to guarantee that most (ideally all) of the participants are represented. At each SB meeting standing items of WP1-7 will be presented by the WP leader. The NC will report any communications from the EC and the T1.4 lead will report from the Advisory Board. Non-reserved minutes will be circulated to all participants and ESRs.

An Advisory Board (AB) will be constituted as an independent assessment body to the SB, to provide external feedback on progress. The initial chair of the AB will be the T1.4 lead, but at the first meeting one of the AB members will be elected as chair, providing independence from the SB. The AB will comprise of three to six external experts and representatives of stakeholders and governmental bodies. If another party is found to be of interest, inviting it to the AB will be considered by the SB. The AB will meet yearly, coinciding with the PriMa Research Events.

3.2.3 Recruitment strategy

Coordination of recruitment of ESRs falls under the responsibility of WP1. Whist the recruitment process will ultimately be implemented by each of individual beneficiaries, *PriMa will adopt a coordinated and centralised selection process across the network, reducing the risk of unfilled ESR posts and the associated delay to the start of a particular ESR project. This method will also ensure consistency in research ability across the network.*

WP1 will develop a set of policies for the recruitment of researchers within the first two months of the network mandating that all beneficiaries adopt the European Charter for Researchers with procedures strictly adhering to the Code of Conduct for Recruitment of Researchers, including the minimum target of hiring at least 40% of female researchers to enhance gender equality. The policies will also include that a gender expert will monitor the recruitment process. All beneficiary institutions within PriMa already adopt these policies for HR/recruitment purposes and hence will be implementing existing procedures. Our network-wide procedures will be open, efficient, transparent, supportive and internationally comparable, tailored to the research position advertised. Our strategy will be to issue a simultaneous call for all ESR positions across the network in Month 3 of the project. Vacancies will be announced using, as a minimum, the following methods:

1. Internet advertising. Via a) PriMa website; b) European Researcher's Mobility Portal Euraxess (http://ec.europa.eu/euraxess/); c) European Associations (e.g. the European Association for Biometrics) and professional networks (e.g., LinkedIn) and paricipants websites; d) Newsletters of the scientific community; e) country specific websites (e.g., http://jobs.ac.uk, https://www.academictransfer.com/).
2. H2020 national contact points and local institution job vacancy portals.
3. Announcements posted at conferences, professional events and standardisation meetings.
4. National female engineering associations and websites related to female researchers.

ESR posts will be advertised with a complete description of the vacancy and the expected profile of the candidate (compulsory requirements and valuable skills) but will not be so specialised as to encourage a wide range of applicants. Each advert will include a description of the working conditions and entitlements, including career development prospects. The time allowed between the simultaneous advertisement of ESR positions and the deadline for reply will be one month - realistic for the candidates and adhering to policies that beneficiaries' HR departments already implement and follow. Applications will be made to a centralised PriMa recruitment email address. This will also be used to vector communication between potential applicants and project supervisors during the recruitment.

A representative of each beneficiary will form a Shortlisting Panel. This Panel will meet via teleconference shortly after the deadline. Applicants meeting the compulsory requirements will be selected and invited to a Selection

Event planned to be held in Brussels in Month 5 (allowing time for visa application, if necessary). Each invitee will be awarded a travel bursary to enable them to attend the Selection Event. At the Event, shortlist candidates will be interviewed by a Selection Panel (comprising of representatives of beneficiaries and parter organisations) and be asked to give a presentation on a topic relevant to the ESR post they have applied for. They will also be asked to undertake a series of teamworking and personality tests. Following the Selection Event, it is envisaged that all ESR posts will be filled, however individual beneficiaries will be able to nominate a reserve candidate from the pool of applicants. An attempt to fill any unfilled ESR positions will also made using the pool of shortlisted candidates. The offer of individual positions will be made through each of the beneficiary's HR departments. By holding the selection event in Month 5 enables sufficient time for the first tranche of ESR positions to commence in Month 7.

During the selection process, gender policies will be considered, as will be institutional policies concerning the recruitment of subjects with refugee status. Each of the beneficiaries' HR policies adhere to EU law in this respect. The composition of the selection committees will bring together diverse expertise and competences, have an adequate gender balance, and, where appropriate and feasible include members from different sectors (academic and non-academic) and disciplines.

3.2.4 Progress monitoring and evaluation of individual projects

At the beginning of their projects, together with his/her supervisor, each ESR will make a Research Plan that will be a part of the ESR's Training and Mobility Plan, describing the global steps that are foreseen in the ESR's research. All ESRs will have weekly meetings with their local supervisors to report on progress in light of the Research Plan and plan next steps. When necessary, these meetings will involve secondment supervisors. The supervisor(s) will review the progress and validate/correct the Research Plan together with the ESR. Monthly, all supervisors will report on the progress of their ESRs to the WP leader in the form of a short report, with the analysis of any deviation in the training and research program and the description of actions to resolve the deviations. The WP leader will check the reports and agree with each of the supervisors on the actions to be taken, if necessary. Finally, WP leaders will report to the SB on the progress to enable the SB to act accordingly. See Section 3.2.1. for procedures to deal with more severe conflict resolution and misconduct. Feedback from ESRs on their training and research process is organised in the training events (See Section 1.2.1).

3.2.5 Intellectual Property Rights (IPR)

It will be mandatory for each beneficiary to sign a Consortium Agreement and for each partner organisation to sign bilateral Partner Agreements with the host beneficiaries of visiting ESRs, covering IPR and non-disclosure. Consortium and Partner Agreements will contain procedures to deal with conflicts (Milestone M1.1 in M01). The principle of not disseminating any method or result that could be filed under a patent until such a patent has been filed will be established in the CA and will be highlighted in the first training event to inform the ESRs. Issues concerning the dissemination of work in scientific journals will be governed by a policy defined within WP3, particularly where joint work is described or work subject to commercial sensitivity. WP3 will define methods for exploiting transfer of technology and the preservation of all IPR and industrial exploitation clauses. The full content of each technology transfer will not be disclosed in order to preserve the confidentiality of such industrial operations, but such a transfer will have to be declared to enable an awareness of the potential IPR issues. The strategy regarding background and foreground knowledge, as detailed at the end of Section 2.3.2, will be part of the Consortium Agreement. WP3 will present directives for best practices in this area in deliverables D3.2 and D3.3.

3.2.6 Gender aspects

Progressing towards gender equality is a main aspect of PriMa to balance the numbers of male and female researchers in this field. As mentioned in the recruitment strategy, PriMa has a minimum target of hiring at least 40% of female researchers and a gender expert will monitor the recruitment process. PriMa will also promote the participation of female scientists as supervisors in training and in management, with the target to reach a participation of at least 40%. Currently, 11% of the supervisors are female. As available and appropriate female staff members will be added to the supervisory teams throughout the project to address this imbalance. Gender balance initiatives such as https://www.utwente.nl/en/ffnt/about/organization/ at UTW are in place at most of the beneficiaries and will be involved to repair the imbalance and to support female ESRs in their career development. A confidential advisor will be identified at UTW as a referee/support for the ESRs in case of sexual harassment at the workplace.

3.2.7 Data management plan

WP3 will produce a Data Management Plan (DMP, D3.5) as part of participation in the Open Research Data Pilot, which will define policies for the management and dissemination of research data and will contain a section on risk management regarding the access to data. WP3 will revise the DMP when necessary. The DMP will contain a data management policy for each ESR, that, as a minimum, will state that databases with personal information acquired within the ESR projects will strictly comply with the regulations by the EU, GDPR and national bodies for data management. If host institutes require individual DMPs for their ESRs, then these will be included in the overall DMP. Before guaranteeing the appropriate level of anonymity, any form of data processing will be forbidden. Only non-identifiable and anonymous data will be shared and used among the consortium members

3.3 Appropriateness of the infrastructure of the participating organisations

All beneficiaries are well-established academic institutes with a proven infrastructure and expertise for the research, supervision and management of local, national and international research projects. Therefore, each beneficiary is able to perform the tasks assigned. In addition, all have independent research and training facilities and are able to conduct the ESR projects without the reliance on third parties. NRS is the only academic beneficiary that cannot award a degree. ESRs hosted by NRS will graduate at NTNU, for which a formal agreement will be made. Across the partner organisations, all are able to host the secondments, and to participate in the training events, providing the training in the transferable skills assigned.

3.4 Competences, experience and complementarity of the participating organisations and their commitment to the programme

3.4.1 Consortium composition and exploitation of participating organisations' complementarities

All beneficiaries have considerable expertise in running and managing educational programmes at an institutional level and have all been involved with major EU research initiatives in the past and are, therefore, ideally placed to run the planned activities. We have, however, devised the responsibilities within the network according to specific skills represented within the consortium: Each of the research WP leaders is an active researcher in the thematic area. UTW has responsibility for recruitment and transferable skills training. UNIKENT has responsibility for mobility within the network recognising the importance of this task. PriMa has specific expertise in overseeing activities relating to dissemination (Spreeuwers, UTW, editorial roles), standardisation (Deravi, UNIKENT, leading EU player) and exploitation (Østvold, NRS, technology transfer). It is important to reiterate we have ensured an even spread across the consortium with tasks allocated according to a work allocation model (Section 1.4.1). Our primary driver for the selection of partner organisations is the support allocated to a specific ESR's project and Career Development Plan. However, the partner organisations also share complementary in that they all have an interest in privacy and security and offer a range of experience, methodologies and requirements.

3.4.2 Commitment of beneficiaries and partner organisations to the program

The beneficiaries in PriMa are academic institutes whose firm commitment is to provide training needed to allow the award of a PhD. As stated, ESRs hosted by NRS, being the only beneficiary that cannot award a degree, will graduate at NTNU. Each beneficiary is also committed to the ethos of the Marie Skłodowska-Curie schemes as a way of enhancing the field of science and technology within an EU context. To achieve this, the beneficiaries will integrate ESRs into their research groups, enabling them to access research facilities, datasets, tools and expertise for their research, thereby maximising the opportunities for successful completion of their PhD. Each beneficiary will provide ESRs with the knowledge and expertise to allow them to build a successful professional career, either in teaching, research, or in the private sector. Partner organisations are committed to provide ESRs with the required complementary training, firstly to direct the research performed in PriMa to viable and applicable results which could be exploited commercially (subject to Technology Transfer and IPR) and secondly to develop experienced researchers that, if suitable, may become part of such organisations in the near future. The stated support position of each of the partner organisations is contained in the letters of support in Section 7 of this proposal.

4. Ethics Issues

The ESR projects in PriMa will address the use of security technologies amongst citizens. This area presents growing opportunities for the commercial market which need to be balanced by recognition of critical ethical, legal and human rights implications.

Many of the ESR projects will use and collect biometric and other personal data. Ethical concerns also relate to issues of the recording of potentially sensitive human attributes (and the associated personal integrity and dignity), as well as to the need to prevent social exclusion and of unauthorised monitoring of biometric profiling – using the data for means not central to the core research. The very critical issue remains the fact that biometric and personal identification systems tend unavoidably to collect extra details about a human subject that can be misused for purposes not linked to citizen approved use. Legal implications are linked to the fact that biometric data are personal data as far as they refer to identifiable persons. Data processing must be undertaken adhering to the main international, EU and national instruments for the protection of privacy and personal data.

Like any innovative technology, these topics need continuous and careful ethical investigation. PriMa will consider the analysis of the legal context and ethical, privacy and data protection principles within the Project Management (in particular T1.3 Data Management of WP1). The need for the consortium to carry out their work with a high level of ethical responsibility is taken very seriously by PriMa and a number of best practice principles will be followed during the development of novel technologies.

In terms of areas for ethical consideration, the work of PriMa will use human participants as volunteers for human sciences research and the collection and/or processing of sensitive personal data. Each of the studies will abide by the following ethical ground rules following the draft proposal for the EU General Data Protection Regulation[89] or the resulting law to be accepted and put into force by the European Parliament. This includes (but is not limited to):

- Subjects will be aged 18 and over.
- Subjects have the right to have their anonymised record removed from the study at any stage.
- Subjects will need to give consent prior to data collection.

Each supervisor and ESR will accept potential participants by identifying their availability. The research team running the trial will advertise locally for participants and/or using databases of subjects available for human research. Subject identity will be anonymised by a random set identifier. Only the research team will have a mapping to real-world identity.

Personal data will be stored only in a secure local server and will *not* be shared by the whole consortium or electronically transferred as such as from one partner to another. Data will be protected with state-of-the-art security and will be used only for the purposes of the present project and then completely erased. When data is required to be shared by multiple partners (for example in joint work) the data will be transferred on an encrypted hard disk and will be hand delivered by the project supervisor as a first resort. No personal data collected will be sold or used for any purposes other than the current project. A data minimisation policy will be adopted at all levels of the project and will be supervised by T1.3 Data Management of WP1. This will ensure that no data that is not strictly necessary to the completion of the current study will be collected. Any data aggregation or categorisation that could be used to discriminate against any particular ethnic, religious or cultural group will be early identified and prevented.

If applicable and appropriate we will make the datasets that have been collected publicly available in accordance with the EU Open Science Initiative to enable reproducibility of scientific results. This will always be done under the explicit written consent of the data subjects and in accordance with national and EU legislation and regulations. Details and procedures will be laid down in the Data Management Plan.

If employees of partner organisations, or university students serving in any partner university, are to be recruited for data collection, specific measures will be in place in order to protect them from a breach of privacy/confidentiality and any potential discrimination. Ethical approval by local Ethics Committees will be obtained prior to the commencement of any data collection involving human participants. Separate ethical approval will be sought through local Ethics Committees at the host institution conducting the research. All partners have significant previous experience in human trials for biometric purposes and so are familiar with produces, best practice and assurances necessary to enable scientific research to proceed. All host institutions within PriMa also have strict policies in place and significant experience in handling the storage of personal research data. These will be adhered to as a

[89] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

condition of local Ethical Approval.

We will produce in T1.3 of WP1 a Data Management Plan as part of participation in the Open Research Data Pilot which will define policy for the management and dissemination of research data. In drafting the Data Management Plan the protection and privacy of an individual will always take precedence over the scientific merit of the release of data to the community. PriMa places absolute reliance on:

- The provision of INFORMED consent by participants, who must know what they are agreeing to take part in and have the capacity to make an informed and reasoned decision. In the case of elderly participants, we must be assured that they have full awareness of their involvement, or that another can take this decision on their behalf.
- The RIGHT TO WITHDRAW. Participants retain the right to withdraw their participation or their data at any stage, before, during and after taking part or providing their behavioural data. This protects the interests of the participations.
- DECEPTION – none of the projects has an element of deception within experimental design.
- DEBRIEF – all participants should be debriefed as to what will happen with their data (including who will see it) and what their data will contribute to in terms of our understanding of identity, behaviour and usability of technologies for all parts of society.

Further to the points outlined above, data gathered as part of the project will fully comply with ethical principles and international, European and national law. In particular:

- EU Directive 95/46/EC[90] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- The new General Data Protection Regulation No. 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – that will apply from May 25th, 2018[91].
- Directive 58/2002/EC[92] of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- European Charter of Fundamental Human Rights[93] and with national data protection legislation, for those countries where testing is taking place.

Human participation

The consortium confirms that all procedures and criteria that will be used to identify/recruit research participants will be submitted as a deliverable.

The consortium confirms that the informed consent procedures that will be implemented for the participation of humans will be submitted as a deliverable.

The consortium confirms that templates of the informed consent and information sheets (in language and terms intelligible to the participants) will be kept on file.

In relation to the activities carried out by ESR4 (NTNU) within PriMa, it is described that: *'...To collect data for research and performance evaluation, social communication mechanisms in real life such as social network and social robot are planned to be utilised to test the models by a series of announced and unannounced experiments compliant to the requirements of the General Data Protection Regulation (GDPR)..'*

It is important to clarify that 'unannounced' in this context means that prior to the experiment a fully informed consent will be given, but that the actual moment of the experiment is not revealed to the subject. Involved humans will receive detailed information on the procedures on experiments. No adults unable to give informed consent will be involved in any of the activities carried out within PriMa.

[90] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[91] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[92] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
[93] http://www.europarl.europa.**eu/charter**/pdf/text_en.pdf

Protection of personal data

The beneficiaries confirm to check if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place and will submit a declaration of compliance with respective national legal framework(s) as deliverable.

Confirmation on Data Protection Officers.
Each beneficiary in PriMa has appointed a Data Protection Officer (DPO) and the contact details of the DPOs – as shown in the table below – will be made available to all data subjects involved in the research.

University of Twente	https://www.utwente.nl/en/cyber-safety/contact/
University of Kent	https://www.kent.ac.uk/outreach/research-and-evaluation/data-protection.html
Norges Teknisk-Naturvitenskapelige Universitet	https://www.ntnu.edu/employees/thomas.helgesen
Norsk Regnesentral	https://www.nr.no/en/homepage/holden
Julius-Maximilians-Universitat Wurzburg	https://www.uni-wuerzburg.de/universitaet/datenschutzbeauftragter/
Katholieke Universiteit Leuven	https://www.law.kuleuven.be/citip/en/staff-members/staff/00055844
Universidad Autonoma de Madrid	https://www.uam.es/UAM/Politica-de-privacidad/1446761787245.htm?language=es

The beneficiaries will explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). This will be submitted as a deliverable.

The consortium confirms that a description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants will be submitted as a deliverable.

The consortium confirms that a description of the anonymysation/pseudonymisation techniques that will be implemented will be submitted as a deliverable.

The consortium confirms that detailed information on the informed consent procedures in regard to data processing will be submitted as a deliverable.

The consortium confirms that templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) will be kept on file.

In case the research involves profiling, the beneficiaries will provide explanation on how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. This will be submitted as a deliverable.

The consortium confirms that an explicit confirmation that the data used in the project is publicly available and can be freely used for the purposes of the project will be submitted as a deliverable.

In case of further processing of previously collected personal data, the consortium confirms that an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organizational measures are in place to safeguard the rights of the data subjects will be submitted as a deliverable.

The beneficiaries will evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 201/679. The risk evaluation and the opinion will be submitted as a deliverable.