Military Data and Information Sharing - A European Union Perspective

Cymutta, S.; Zwanenburg, M.; Oling, P.

DOI
10.23919/CyCon55549.2022.9811028
Publication date
2022
Document Version
Final published version
Published in
2022 14th International Conference on Cyber Conflict: Keep Moving

Published by CCDCOE

2022

14th International Conference on Cyber Conflict: Keep Moving

T. Jančárková, G. Visky,
I. Winther (Eds.)

CYCON

IEEE
Advancing Technology for Humanity

2022
14TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: KEEP MOVING

IEEE Catalog Number: CFP2226N-PRT
ISBN (print): 978-9916-9789-0-0
ISBN (pdf): 978-9916-9789-1-7

COPYRIGHT AND REPRINT PERMISSIONS

CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Layout: JDF

2022 14th International Conference on Cyber Conflict
Keep Moving
T. Jančárková, G. Visky, I. Winther (Eds.)

Military Data and Information Sharing – a European Union Perspective

Sebastian Cymutta*
Law Researcher
NATO CCDCOE
Tallinn, Estonia
sebastian.cymutta@ccdcoe.org

Marten Zwanenburg*
Professor of Military Law
University of Amsterdam and
Netherlands Defence Academy
Amsterdam, Netherlands
m.c.zwanenburg@uva.nl

Paul Oling*
PhD candidate Intelligence & Security
Netherlands Defence Academy
Breda, Netherlands
p.oling@mindef.nl

Abstract: The use of biometric data during and beyond military operations has become a top priority for the North Atlantic Treaty Organization (NATO) in recent years. But biometrics has also been relevant for European Union (EU)-led operations. The use of biometrics in multinational operations, particularly the sharing of biometric data, raises important legal questions. This is particularly the case for EU-led operations, which operate in the framework of an organization that has a strong focus on the protection of the right to privacy and on data protection.

This paper intends to address legal questions surrounding the use of biometric data for different purposes in the course of a multinational military operation, with a focus on EU-led operations. The article has a special emphasis on the sharing of biometric data, both between (EU member) States and between domains.

Keywords: *biometrics, Common Security and Defence Policy (CSDP), data protection, European Union law, fundamental rights, 'Ping + Ring'*

* The views expressed in this article are the authors' alone and do not reflect the official position of any organization they might be working for.

1. INTRODUCTION

The use of biometric data for the purpose of verification or identification has become widespread in today's society. Unlocking a smartphone via fingerprint or passing airport security using facial recognition are examples of biometric verification. Searching a biometric database to connect a latent fingerprint to a known criminal is an example of biometric identification.

Simultaneously, biometric technology is increasingly adopted in the area of military intelligence and security due to its potential to strip adversaries of the advantage of anonymity. Military adoption of biometrics has already led to its use in a number of multinational operations, such as during North Atlantic Treaty Organization (NATO)-led military operations in Afghanistan and operations in Iraq.[1]

The use of biometric systems in European Union (EU)-led missions is far less common and has received little attention so far. Considering the potential benefits of this technology in a military environment, it is likely that there will be a push for more widespread use within such missions. An example of this development is the EU-led operation EUNAVFOR MED IRINI. Established in 2020, its primary task is enforcing the United Nations arms embargo on Libya, to which end the mission may 'collect and store, in accordance with applicable law, personal data concerning persons involved in the carriage of such prohibited items related to characteristics likely to assist in their identification, including fingerprints'.[2]

This article focuses on the application of EU legislation concerning data protection to the sharing of biometric data within EU-led military missions. The use of biometrics is more prevalent in NATO-led operations than in EU-led missions. This is mainly a consequence of the fact that the United States, which is at the forefront of military use of biometrics, is part of NATO and not the EU. Unlike NATO, the EU is unique as an international organization, in that it has developed an extensive framework for the protection of data, including biometric data. This raises expectations concerning legal safeguards when using biometric systems in military missions led by the EU, especially with respect to the sharing of biometric data. Against this background, this article discusses how the EU data protection framework impacts the processing and sharing of biometric data in the context of EU-led missions. It may be noted, however, that the conclusions of this article may also be relevant for NATO operations, as many EU member States are also members of NATO and may be bound by EU data protection law when taking part in NATO operations.[3]

1 Annie Jacobsen, *First Platoon: A Story of Modern War in the Age of Identity Dominance* (Penguin 2021).
2 Council Decision (CFSP) 2020/472 of 31 March 2020 on a European Union military operation in the Mediterranean (EUNAVFOR MED IRINI) [2020] OJ L101, arts 2(6) and 4(5).
3 This is the case in any event for those EU and NATO member States that have domestic legislation that makes EU data protection law or parts thereof applicable to their armed forces. See section 3 below.

The article is structured as follows: after this introduction, section 2 provides a brief introduction to EU military missions and the use of biometric data. Section 3 gives an overview of the EU legal framework pertaining to data protection. This framework will be applied to biometric data sharing in the Common Security and Defence Policy (CSDP) domain in section 4. To provide some more insight into the concrete application of the relevant law, this section includes a discussion of several cases of such sharing. The article concludes with a number of final remarks.

Limitations on the use of biometric data and information sharing in EU-led missions may also follow from the application of the European Convention on Human Rights (ECHR), to which all EU member States are parties. Owing to space constraints, the application of the ECHR will not be addressed in this article.[4]

2. EU MILITARY MISSIONS AND THE USE OF BIOMETRIC DATA

A. The EU as a Military Actor

Since the new millennium, the EU has taken up a much more active role when it comes to military endeavours, starting in 2003 with the first EU military operation Concordia in what is now North Macedonia.[5] As of March 2022, the EU was conducting 7 military missions as well as 11 civil missions,[6] sometimes within (or near) the same region as military operations conducted by NATO.[7]

The need for a military endeavour usually arises in regions that are not only far less economically developed than the EU member States, but also are considerably more dangerous. Indeed, over the years, EU military missions have frequently been deployed to volatile regions. One example of this is the European Union Training Mission in Mali, which has seen a number of incidents.[8]

4 See for more on this topic e.g. Steven van de Put and Marten Zwanenburg, 'Military Use of Biometrics and the Right to Private Life in Article 8 ECHR' (working title) [2022] NL ARMS (forthcoming).

5 Council Joint Action 2003/92/CFSP of 27 January 2003 on the European Union military operation in the Former Yugoslav Republic of Macedonia [2003] OJ L 34; see generally on the development of EU military endeavours Sabine Mengelberg, 'Permanent Change: the Paths of Change of the European Security Organizations' (PhD thesis, Leiden 2021).

6 See for more information, 'Military and civilian missions and operations' (European Union, 5 March 2019) <https://www.eeas.europa.eu/sites/default/files/eu_csdp-missions-and-operations_2021-10.pdf> accessed 12 April 2022.

7 For example: EULEX in Kosovo and KFOR / EUAM Iraq and NATO Mission Iraq.

8 See e.g. Deutsche Welle, 'Gunmen Attack Bamako Base of EU Military Training Mission in Mali' (Berlin, 21 March 2016) <https://www.dw.com/en/gunmen-attack-bamako-base-of-eu-military-training-mission-in-mali/a-19132542> accessed 2 March 2022; Associated Press, 'EU Training Mission Comes under Attack in Mali' (New York City, 14 February 2019) <https://apnews.com/c375c2a0628b43d286c71ef06f5fb89f> accessed 2 March 2022.

B. The EU's Common Foreign and Security Policy

EU military missions are conducted within the intergovernmental[9] framework of the Common Security and Defence Policy (CSDP), which is a subcategory of the EU's Common Foreign and Security Policy (CFSP). The legal basis for the CFSP is found in Title V of the Treaty on European Union (TEU). Articles 42(1) and 42(3) TEU provide the EU with an operational capacity drawing on civilian and military assets of the member States. The EU may use these assets for 'missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter'.[10]

Whereas Article 42 TEU refers only to 'missions', it is common to refer to 'operations' when talking about executive or military endeavours and to 'missions' when talking about non-executive endeavours. For ease of reference, this article will use the term 'mission' to refer to both operations and missions.

An important assumption in this article is that biometric data collected by a participating State in an EU-led mission is 'owned' by that State, and not by the EU. This is how the issue of 'ownership' is approached in NATO missions and we do not see a need to take a different approach in the context of EU-led missions.[11]

C. Biometrics and the 'Ping & Ring' Concept

'Biometrics' or 'biometric recognition' is defined as the automated recognition of individuals based on their biological and behavioural characteristics.[12] It uses the physical, physiological and/or behavioural characteristics of individuals to recognize them.[13] Examples of such characteristics are face topography, hand topography, finger topography, iris structure, vein structure of the hand, voice, gait, and DNA.[14] These characteristics are unique, which makes them very suitable for recognizing persons.[15]

A 'biometric system' is defined as a system for the purpose of biometric recognition of individuals based on their behavioural and biological characteristics.[16] It is essentially a pattern recognition system that operates by acquiring biometric data from an

9 Grabitz/Hilf/Nettesheim/Kaufmann-Bühler EUV art 42 paras 13, 14.
10 Treaty on European Union (Maastricht Treaty) art 42(1).
11 Hence this paper does not discuss the data protection rules pertaining to EU bodies and institutions and therefore does not consider Regulation (EU) 2018/1725, seeing that this body of law explicitly excludes itself from being applicable to entities created according to articles 42(1), 43, 44 TEU.
12 ISO/IEC International Standard 2382-37, *Information Technology – Vocabulary – part 37: biometrics* 2 (2012).
13 See for an extensive description of biometrics inter alia Nancy Y Liu, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics* (1st edn Routledge, 2012) 29–59.
14 For additional characteristics see William H Boothby, 'Biometrics' in William H Boothby (ed) *New Technologies and the Law in War and Peace* (Cambridge University Press 2019), 192.
15 'Recognizing' is used here as a term encompassing verification and identification as defined below.
16 ISO/IEC International Standard 2382-37 (n 12).

individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.[17]

The use of biometrics in multinational military operations may take the shape of biometric 'ping & ring networks'. The 'ping & ring' concept involves biometric data queries which, when matched in certain databases, yield a reference number and a point of contact for follow-on bilateral action.[18] Personnel from one State may send biometric data to another State and request that the other State use the data to run a query in their biometric database. The query does not give them direct access to the actual biometric data in the database, or to the biometric data subject's biographic or contextual data. If there is a match, the State that made the request may ask for more information. In other words, a query in a ping & ring network involves the requesting State sharing biometric data. The sharing of data from the database by the requested State may follow on a bilateral basis if there is a match.

D. The (Potential) Role of Biometric Data Sharing

Military organizations increasingly face adversaries that 'simultaneously and adaptively employ a fused mix of conventional and improvised weapons, irregular tactics, terrorism and criminal behaviour in the battlespace to obtain their political objectives'.[19] A striking example is the insurgents' use of Improvised Explosive Devices (IEDs), the signature weapon of recent asymmetric conflicts in Iraq, Afghanistan, Mali and Syria. Unexpected external shocks, such as the IED threat faced in Iraq and Afghanistan, are 'fertile ground for innovation'.[20] To counter the threat of IEDs, military organizations utilize emerging technologies pertaining to the intelligence and security domain.

Initially, most counter-IED (C-IED) efforts focused on defensive security technologies, such as improved armoured plating and tactics, techniques, and procedures to detect IEDs.[21] Over time, C-IED efforts became more proactive with an emphasis on intelligence.[22]

The use of biometrics by military organizations is an example of both strategies. Biometric technology was deployed in Kosovo as part of the counter-intelligence activities to grant authorization to individuals accessing military bases.[23] In Iraq and

17 Anil K Jain, Arun Ross and Salil Prabhakar, 'An Introduction into Biometric Recognition' (2004) 14 IEEE Transactions on Circuits and Systems for Video Technology 4, 5.

18 Victor Morris, 'Identity and Biometrics Enabled Intelligence (BEI) Sharing for Transnational Threat Actors' (2016) Small Wars Journal.

19 Frank Hoffman, '"Hybrid Threats": Neither Omnipotent Nor Unbeatable' (2010) 54 Orbis 441.

20 Adam Grissom, 'The Future of Military Innovation Studies' (2006) 29 Journal of Strategic Studies 905.

21 David W Barno and Nora Bensahel, *Adaptation under Fire: How Militaries Change in Wartime*. Bridging the Gap (Oxford University Press 2020).

22 Theo Farrell, Frans PB Osinga and James A Russell, *Military Adaptation in Afghanistan* (Stanford University Press, 2013).

23 Jacobsen (n 1) 48.

Afghanistan, coalition forces increasingly relied on biometrics as an offensive tool, supporting biometrics-enabled intelligence. Biometrics were used to link persons to times, locations, groups and activities, while simultaneously providing a means to detect and identify them in the future. Forensically exploiting IED components or remnants, documents and electronic data carriers allowed for the identification and disruption of networks of individuals supporting the IED threat.

As these networks are not restricted by artificially defined operational areas within a theatre, exchanging biometric data within a multinational mission is vital. Or as described by Arquilla et al., 'it takes a network to defeat a network'.[24] This intense cooperation during a multinational mission may lead to isomorphism between military organizations, where organizations try to emulate one another.[25]

However, using a solely deterministic approach to the introduction of biometrics does not adequately take into account the influence of societal acceptance of a technology on its use by military organizations. The acceptance of the use of biometrics at home shapes the approval for military use abroad. Moreover, the way a nation allows its military to use biometrics shapes the way technical interoperability between military organizations is achieved. For example, legal caveats for data retention – when applicable – must be made part of the technical interoperability, accompanying exchanged biometric data from the cradle to the grave. As the United States may be considered a pacesetter for the military application of biometrics, their societal acceptance of the technology and its legal safeguards resulting from that is reflected in current military-technical standards on interoperability.

3. THE LEGAL FRAMEWORK OF THE EU PERTAINING TO DATA PROTECTION

A. Primary Law Implications

Article 39 TEU is a statutory source for CFSP-specific rules on data protection.[26] It refers to Article 16 of the Treaty on the Functioning of the European Union (TFEU) and tasks the Council with the adoption of legislation laying down the rules relating to the protection of individuals with regard to the processing of personal data by the member States when carrying out activities which fall within the scope of the chapter in the TEU dealing with the CFSP, and the rules relating to the free movement of such data.

24 John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND Corporation 2001).

25 Theo Farrell and Terry Terriff (eds), *The Sources of Military Change: Culture, Politics, Technology, Making Sense of Global Security* (Lynne Rienner Publishers 2002).

26 Calliess/Ruffert/Kingreen EU-Vertrag (Lissabon) (2022) art 39 para 1; Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV/von Heinegg EUV (2017) art 39 para 2.

Article 39 highlights for the first time[27] that the CFSP is not a data protection-free area of EU policy and action, drawing on the material provisions of Article 16 TFEU. While Article 16 is the most prominent provision regarding data protection in EU primary law, Article 8 of the EU Charter of Fundamental Rights (CFR) further emphasizes the concept of data protection as a human right.[28] While technically not considered part of the primary law of the EU, the CFR is recognized by the EU and has the same legal force as the Treaties.[29] Article 8(1) CFR provides that 'everyone has the right to the protection of personal data concerning him or her'. In its second subsection, it is further stipulated that 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law and that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. The objective of this fundamental right, it is suggested, is to protect an individual's control over personal data.[30]

Article 8 CFR is based in part on Directive 95/46/EC 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 (Directive 95/46/EC), the forerunner of Regulation (EU) 2016/679 of the European Parliament and of 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 (General Data Protection Regulation (GDPR)).[31] It is submitted that for this reason, Directive 95/46/EC and the GDPR as its successor may be instructive in establishing what Article 8 CFR requires.[32]

Since Article 51 CFR limits the Charter's scope of application to the member States only when implementing Union law, it begs the question whether the armed forces of a member State participating in a CSDP mission would qualify as 'implementing Union law'. Naert has rightly argued that this is indeed the case. This is because 'implementing Union law' encompasses situations in which member States implement

27 Thomas Ramopoulos, 'Article 39', in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019) 1159.

28 Charter of Fundamental Rights of the European Union [2012] OJ C326/02.

29 See art 6(1) TEU.

30 Tobias Lock, 'Article 8 CFR', in Kellerbauer et al (n 27) (2019) 2123.

31 Directive 95/46/EC 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 [1995] OJ L281; Regulation (EU) 2016/679 of the European Parliament and of 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 (General Data Protection Regulation) [2016] OJ L119.

32 See Herke Kranenborg, 'Article 8', in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart 2014) 223, 247.

Council acts setting up EU military operations, as such decisions are legal (albeit not legislative) acts under EU law.[33]

Article 52 CFR allows for derogations from the rights set out in the CFR. However, any limitation must be provided for by law, and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.

B. Secondary Law Implications

1) The Need for Concretization

While EU primary law contains some strong fundamental rights with regard to data protection, these rights are largely dependent on being substantiated by EU secondary law. This holds true especially for the CFSP domain. Even though the fundamental right of data protection is applicable within the CFSP, the primary law of the EU recognizes that the peculiarities of the CFSP (and especially the CSDP) warrant a different kind of data protection regime than the one established on the basis of Article 16(2.1) TFEU for the civilian sector.[34] It is Article 16(2.2) TFEU that recognizes the need for specific rules laid down by Article 39 TEU for the CFSP. Hence, Article 39 TEU in conjunction with Article 16 TFEU obliges[35] the Council to enact a special data protection regime that takes into account the unique circumstances of endeavours undertaken within the CFSP.[36] Unlike in Article 16 TFEU, the European legislator does not enjoy freedom of choice with regard to the secondary law instruments provided in Article 288 TFEU. Article 39 TEU calls for a decision in the sense of Article 288(4) TFEU, which 'shall be binding in its entirety'.

2) Filling the Gap

Despite the above-mentioned obligation to do so, the Council has adopted no decision so far. Since a gap in secondary legislation is undesirable, mitigation might be achieved by applying existing EU data protection legislation.[37]

33 Frederik Naert, 'Shared Responsibility in the Framework of the European Union's Common Security Defense Policy Operations' in André Nollkaemper and Ilias Plakokefalos (eds), *The Practice of Shared Responsibility in International Law* (Cambridge University Press 2016); Carmen Márquez Carrasco, 'Human Rights in the EU's Common Security and Defence Policy', in Jan Wouters, Manfred Nowak, Anna-Luise Chané and Nicholas Hachez (eds), *The European Union and Human Rights: Law and Policy* (Oxford University Press 2020) 408, 415.

34 Most notably the GDPR (n 31) and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295.

35 Streinz/Regelsberger/Kugelmann EUV (2018) art 39 para 1.

36 Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV/von Heinegg EUV (2017) art 39 para 3.

37 Grabitz/Hilf/Nettesheim/Kaufmann-Bühler EUV (2021) art 39 para 5.

The GDPR is the most influential secondary law act in the area of data protection. However, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data is lex specialis in relation to the GDPR, as far as the protection of natural persons specifically with regard to the processing of personal data for law enforcement purposes is concerned.[38]

What the Regulation and the Directive have in common is that their scope of application does not extend to data processing 'in the course of an activity, which falls outside the scope of Union law'.[39] In addition, the GDPR does not apply to data protection activities by the member States 'when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU'.[40] Consequently, neither the GDPR nor Directive 2016/680 can provide a fully applicable data protection regime for CSDP-missions. Yet in this context, it is important to note that a number of EU member States have unilaterally extended the application of the GDPR[41] or enacted comparable legislation[42] to govern the activities of their armed forces. Hence, it is fair to say that at least some of the provisions of the GDPR were considered to be a good fit for the needs of these States, when trying to establish a data protection regime for their militaries. Therefore, this paper will approach the idea of applying the GDPR / Directive 2016/680 by way of analogy, when assessing biometric data sharing within the CSDP-domain.

4. BIOMETRIC DATA SHARING IN THE CSDP DOMAIN

In this section, the framework set out in section 3 will be applied to biometric data sharing in the CSDP domain. Subsections C to E discuss several cases of such sharing, providing insight into the concrete application of the relevant law.

38 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119.

39 See Directive 2016/680 (n 38), art 2(3)(a) and GDPR (n 31) art 2(2)(a).

40 See GDPR (n 31), art 2(2)(b).

41 Sebastian Cymutta, 'Biometric data processing by the German armed forces during deployment' (2021) CCDCOE, 7–8.

42 For example, the Netherlands has implemented the Uitvoeringswet Algemene Verordening Gegevensbescherming and Regeling Gegevensbescherming Militaire Operaties.

A. Utilizing the GDPR

As it is directly applicable to the CSDP, Article 8 CFR will be the primary reference point when assessing the legality of biometric data processing,[43] which includes sharing, in EU military missions.

It follows from the second paragraph of Article 8 CFR that the sharing of biometric data requires either the consent of the person concerned or some other legitimate basis laid down by law. Consent must be understood as informed consent.[44] If consent has not been given, sharing is still possible if there is another legitimate basis, but only if this is laid down by law. As was already stated, Article 8 CFR is based in part on Directive 95/46/EC, the forerunner of the GDPR. It is submitted that for this reason, Directive 95/46/EC and the GDPR as its successor may be instructive in establishing what Article 8 CFR requires.[45]

For the purposes of this paper, Article 9 GDPR is of particular importance, as it contains specific rules on the processing of special categories of personal data, including biometric data, for the purpose of uniquely identifying a natural person.[46] According to this provision, the processing of biometric data is in general forbidden, except in the cases provided for in Article 9(2) GDPR. Of particular interest for CSDP missions is Article 9(2)(g), according to which processing could be allowed 'if it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'. This very high standard is reflective of the sensitive nature of biometric data, and while Article 9 does not directly apply to CSDP missions, it is reasonable to assume that a similarly high standard applies under Article 8 CFR.

B. Legal Principles Influencing Biometric Data Sharing

Legislation allowing for the processing of data must lay down clear and precise rules governing the scope and application of measures, and its application should be foreseeable to persons subject to it.[47] It should also impose minimum safeguards concerning duration, storage, access for third parties, procedures for preserving the integrity and confidentiality of data and for its destruction, as well as sufficient

43 Processing is very broadly understood as to include 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction', see GDPR (n 31), art 4(2).

44 Norbert Bernsdorff, 'Artikel 8' in Jürgen Meyer (ed), *Charta der Grundrechte der Europäischen Union* (3rd edn, Nomos 2010) para 21.

45 See Kranenborg (n 32) 247.

46 GDPR (n 31) art 9(1).

47 GDPR (n 31) recital 41.

guarantees against the risk of abuse and arbitrariness.[48] In particular, the automatic processing of data increases the need for such safeguards.[49]

It follows from Article 8 CFR that the sharing of data may only be done for specified purposes. Although this is not explicitly stated, it is submitted that this includes the applicability of the 'purpose limitation principle' or 'finality principle', which is one of the cornerstones of data protection.[50] This principle, which is also set out in Article 5(1)(b) of the GDPR, requires that data should not be further processed in a way that is incompatible with the purposes for which it was originally processed (subject to limitations allowed under Article 52 CFR).

The principles of necessity and proportionality are also fundamental elements of data protection. They are referred to in Article 5(1)(c) of the GDPR. This provision states that personal data should be 'adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimisation")'. Necessity requires that if less intrusive means can achieve the same purpose, personal data may not be processed.

Proportionality requires an assessment of the impact of the right to personal data protection against the constitutional value it aims to achieve. To ascertain whether interference is disproportionate, it is necessary to consider how the right to data protection will be restricted – for instance, the type of data that will be processed and whether it involves specially protected data – and the safeguards in place.[51]

Transparency is another important principle of data protection. It is reflected in Article 5(1)(a) GDPR, which provides, inter alia, that personal data shall be processed 'in a transparent manner in relation to the data subject'. The transparency of data processing is part of what constitutes 'fair' processing, as referred to in Article 8 CFR.[52]

C. Base Access and Data Transfer

As far as the authors are aware, EU missions have not yet used biometrics in the context of base access. However, this could change in the future, as this has become a common methodology in the last decade. It has also been suggested that in order to be truly effective, a biometric access control system should be able to exchange data with the biometrics systems being used by operational forces, and that an access control

48 ibid; see also Lock (n 30), referring to *S and Marper v UK* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 99.

49 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] para 55.

50 See Kranenborg (n 32) 247.

51 Antonio Troncoso Reigada, 'The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing' (2012) 17 Lex Electronica 2, 18.

52 Kranenborg (n 32) 254.

system should be able to use the same biometric watch list being used by forces in the field.[53]

It follows from the above that such sharing of data would require explicit consent or another legitimate basis laid down in law. To the extent that consent for sharing their data would be requested from persons being enrolled in the biometric system, such consent must be freely given. It may be questioned, however, whether this is possible under the circumstances. Recital 43 of the GDPR provides that 'in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation'.

Such a power imbalance is clearly present in relations between a military operation and local personnel seeking access. As to the presence of another legitimate basis, such a basis must be laid down in law. This is arguably the case for member States that have domestic legislation concerning biometrics in military operations, such as the Netherlands and Germany.[54] For States that do not have such national legislation, the question is whether an international legal basis for the operation is sufficient. This could be either the EU Council Decision that forms the basis for the mission under EU law, or the legal basis under general international law, for example, a document setting out the consent of the host State to the mission or a Resolution of the United Nations (UN) Security Council under Chapter VII of the UN Charter. Arguably, the wording of Article 8 CFR does not exclude the possibility that such sources (EU or international) of law satisfy the 'laid down in law' criterion. However, such instruments would need to meet high standards that set out clear and precise rules governing the scope and application of measures and impose minimum safeguards concerning duration, storage, access for third parties, procedures for preserving the integrity and confidentiality of data and for its destruction as well as sufficient guarantees against the risk of abuse and arbitrariness.[55] It seems clear that the mere granting by the UN Security Council of the power to 'use all necessary means' to achieve the mission's mandate, for example, would not meet these requirements.

The 'transparency principle' sets high standards for the communication between the member State collecting biometric data for controlling base access and the data subject. At the very least, it requires that information be made available in a language that the local population understands. Furthermore, it may be wondered whether it is feasible in a CSDP mission to provide data subjects with access to their personal data, which is required by the transparency principle.

53 William C Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield* (1st edn, CRC Press 2017) 49–50.
54 See section 3B above.
55 See section 4B.

D. Biometric Data Sharing in Theatre

The 'purpose limitation principle' requires that the transfer of biometric data be limited to the purposes for which the data was originally collected. Arguably, this would allow the sharing of data collected in the context of base access with other States within the mission, as long as the transfer was for the purpose of ensuring the protection of the personnel of the mission, if this was defined as the purpose for collecting biometric data in the context of controlling base access. Protection of the personnel of the mission is a vital requirement for the mission to be able to fulfil its mandate.

With regard to the sharing of biometric data with States outside the mission, the case-law of the European Court of Justice (ECJ) with regard to the EU–Canada Passenger Name Record agreement suggests that it will be very difficult to find an adequate legal basis for sharing outside the mission. In that case, the ECJ rejected the grounds of 'protection of public security against terrorism and serious transnational crime' as a legal basis for sharing sensitive personal data.[56]

It has been argued that the general protection of personal data laid down in Article 8(1) CFR places limits on the transfer of data to third countries.[57] It is noted that this article assumes that biometric data is 'owned' by States when personnel of the State concerned participate in a mission led by an international organization. Consequently, the limits referred to above also apply to the transfer of data between (States participating in) EU-led missions and (States participating in) another mission, such as those led by NATO. To understand what the sharing of data with another State requires, it is informative to look at how this has been operationalized in the GDPR. Under that regulation, transfer of personal data to another State may only occur where that State affords 'adequate protection' of such data. This means that the protection guaranteed in the third country concerned must be 'essentially equivalent' to that under EU law.[58] The legal order of the third country must effectively protect the right to personal data, which includes clear limits to interferences with such data – concerning access, use, and so on – and procedural safeguards in place.[59]

According to the ECJ, the transfer of 'sensitive data' – such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership – 'requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime'.[60] In the case in which the ECJ set out this standard, concerning an envisaged agreement

56 Opinion 1/15, *Transfer of Passenger Name Record data from the European Union to Canada* [2017] ECLI:EU:C:2017:592, para 165.
57 Lock (n 30) 2126.
58 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 73.
59 ibid paras 79–98.
60 Opinion 1/15, *Transfer of Passenger Name Record data from the European Union to Canada* (n 56) para 165.

between the EU and Canada, biometric data was not involved. If it had been, in view of the special nature of biometric data, it is highly likely that the ECJ would have applied similarly high standards to the sharing of such data with another State.

Finally, Article 8(3) CFR requires the existence of a surveillance authority in each member State. The purpose of such an authority is to ensure the effectiveness and reliability of monitoring compliance with the law on the processing of personal data. Its aim is to strengthen the protection of individuals.[61]

In conclusion, based on an interpretation of Article 8 CFR using the GDPR and Directive 2016/680 by analogy, the sharing of biometric data in theatre requires establishing many safeguards. It is submitted that the ping & ring concept discussed before may allow for the integration of many of those safeguards.

E. Military-Civilian Data and Information Sharing

Another challenge would be the sharing of biometric data with other EU authorities. Exceptions aside, the purposes for which those authorities would use the data would most likely not be related to the purposes of the EU mission in the context of which the data was collected.

An example is EUNAVFOR MED IRINI,[62] which is currently operating in the South Central Mediterranean Sea under a mission mandate that aims to contribute to the disruption of the business model of human smuggling and trafficking networks and, not least of all, enforcing a UN arms embargo imposed on Libya.[63] To facilitate this, IRINI is allowed to collect personal data (including biometric data) and store it.[64]

Without negating the military character of IRINI, it is understood that the mandate is closely aligned to law enforcement efforts and that the biometric data collected during the mission is of interest and importance for EU law enforcement agencies. Hence, the EU Council Decision establishing IRINI provides for the transfer of this data to the relevant law enforcement authorities of member States and to competent Union bodies in accordance with applicable law.[65]

In the absence of a Council Decision detailing the (technical) rules relating to the processing (sharing) of personal data within the CFSP, the present reference to the 'applicable law' allows for a fallback to Article 8 CFR and the application by analogy of the provisions of the GDPR and Directive 2016/680. Arguably, for missions like IRINI, which have many characteristics of law enforcement operations, Directive

61 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (n 58) para 41.
62 Council Decision (CFSP) 2020/472 (n 2); IRINI is the successor-mission to EUNAVFOR MED Sophia, which was established by Council Decision (CFSP) 2015/778 of 18 May 2015 on a European Union military operation in the Southern Central Mediterranean (EUNAVFOR MED) [2015] OJ L122/31.
63 ibid art 1.
64 ibid arts 2(6) and 4(5).
65 ibid.

2016/680 would be the most appropriate analogy. However, as was mentioned above, several EU member States have made the GDPR applicable to military operations through domestic legislation. This suggests that they consider the GDPR as providing an appropriate basis for the regulation of the use of biometrics by military missions. This is why the remainder of this section will refer to the GDPR.

Under the GDPR regime, while the collection of fingerprints would have to be measured against the underlying intention of Article 9 GDPR, the collection and storage could be considered legal under Article 9(2)(g).[66] It can be argued that the investigation and prosecution of persons involved in arms smuggling to Libya and human smuggling is a 'substantial public interest'. In that case, processing of biometric data would be allowed, provided that suitable and specific measures to safeguard the fundamental rights and the interests of the data subject have been taken. As there is no public information regarding how the processing of data collected in the context of IRINI takes place in general, it cannot be determined whether this requirement has been met.

However, that leaves the question of whether or not this biometric data can legally be shared with 'competent EU bodies' in the light of the principle of purpose limitation, as discussed above. It is submitted that a transfer of personal data from IRINI to another EU institution would constitute 'further processing' in the sense of Article 6(4) GDPR, and hence would have to be measured against a high standard. In practice, IRINI has concluded a Working Arrangement with the European Border and Coast Guard Agency (Frontex), detailing their cooperation[67] and focusing on 'cross-border crime such as arms trafficking and the disruption of the human smuggling model and trafficking networks'.[68]

This Working Arrangement details the Exchange of Information (and personal data) between IRINI and Frontex in section 5, where it provides for the (analogous) applicability of the GDPR and Article 8 CFR. This underlines the argument that in the absence of a Council Decision detailing data protection rules especially for the CFSP, referencing Article 8 CFR and the GDPR is a suitable workaround.

Therefore, this article argues that while the transfer of biometric data from IRINI to

66 Cymutta (n 41) 9.

67 A similar Working Agreement has been concluded between EUNAVFOR MED Sophia and EUROPOL, see 'Working Arrangement establishing cooperative relations between EUNAVFOR MED Operation Sophia and Europol' (EUROPOL, 16 January 2016) <https://www.europol.europa.eu/partners-collaboration/agreements/working-arrangement-establishing-cooperative-relations-between-eunavfor-med-operation-sophia-and-europol> accessed 2 March 2022.

68 See 'Working Arrangement between The European Border and Coast Guard Agency (Frontex) and EUNAVFOR MED IRINI' (Frontex, 18 January 2021), s 2(2), the conclusion of this kind of Working Agreements is foreseen in art 68(1)(j) of Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L295; the predecessor mission 'Sophia' contained a corresponding provision in Council Decision 2015/778 (n 69) art 8(3).

Frontex is permissible on the basis of the instruments in place, its legality has to be measured against standards similar to the strict standards of Article 9(2)(g) GDPR.

5. CONCLUSION

This article discussed how the EU data protection framework impacts the processing and sharing of biometric data in the context of EU-led missions. In the absence of a decision by the Council as required by Article 39 TEU, the data protection regime that applies to such missions is not clearly defined. Understanding and developing the data protection regime pertaining to EU military missions is important for those carrying out such missions, and also to foster legal interoperability within a CSDP mission and beyond. As an example of interoperability beyond CSDP missions, there is likely to be increased cooperation between the EU and NATO in the future.

Whether it be the exchange of personal data between the member States, the enrolment of locally employed persons for granting base access or the sharing of personal data with bodies outside of the CSDP mission, all of these actions concern the (universal) right of data protection as it is provided for by the primary law of the EU.

While a comprehensive Decision of the Council detailing the rules for the processing of personal data in the CFSP is still missing, this paper showed that an acceptable standard of data protection (procedure) could be based on Article 8 CFR and the analogous application of certain provisions of the GDPR. Further legal substance would be given to these standards through agreements with the entities with which biometric data is shared, either through agreements with States or through 'Working Arrangements' with EU institutions. While this legal workaround appears to live up to practical needs, negotiating one or more (Working) Arrangements for each CSDP mission, potentially with several different States and EU institutions,[69] appears likely to be time-consuming and would potentially lead to new obstacles regarding legal interoperability. Seeing that EUNAVFOR MED IRINI recently struck another Working Arrangement with the EU Border Assistance Mission in Libya,[70] there is also a danger of the legal landscape fragmenting further. A comprehensive Decision on the basis of Article 39 TEU could not only eliminate the need for these kinds of Working Arrangements but could also provide adequate guidance for sharing personal data collected by CSDP missions with other security regimes like NATO or the UN, effectively contributing to international legal interoperability.

69 In addition to Frontex, it is also conceivable that European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) could be interested in receiving personal data collected during EU military operations.

70 See EUNAVFOR MED operation IRINI, 'Best practices, information & integrated approach. Operation EUNAVFOR MED IRINI signs a working arrangement with EUBAM Libya' (European Union, 7 August 2021) <https://www.operationirini.eu/best-practices-information-integrated-approach-operation-eunavfor-med-irini-signs-working-arrangement-eubam-libya/> accessed 2 March 2022 (as of March 2022 the text of the working arrangement was not available.