CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

# Biometric data processing by the German armed forces during deployment

Sebastian Cymutta
**NATO CCDCOE Law Researcher**

Tallinn 2021

# Table of Contents

# 1. Introduction

This paper examines the legal requirements for the processing of biometric data by the German armed forces (Bundeswehr), taking into account European and national regulations. The aim is to identify the legal determinants of this special domain of data protection law and to make it usable for further research.

Since a deployment of the Bundeswehr is usually extraterritorial, the question of the applicability of national regulations outside of the territory of the Federal Republic of Germany must be asked in this context. This is all the more true since the ground-breaking ruling by the Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) on international-foreign telecommunications intelligence by the Federal Intelligence Service (Bundesnachrichtendienst, BND)[1].

## 1.1 International developments

While the processing of biometric data in everyday life or the private sector has often been the subject of jurisprudence and legal research, questions of data protection in the Bundeswehr have only occasionally been referred to the legal discourse.[2] Therefore, it is not surprising, that there has not yet been a specific investigation into the processing of biometric data by the Bundeswehr. However, a closer look at this topic is necessary, considering international developments.

The United Nations Security Council enacted United Nations Security Council Resolution (UNSCR) 2396/2017[3] deciding the following:

> 'Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law'.

Also the North Atlantic Treaty Organization (NATO) has increasingly focused on using biometric data in multinational operations. The Brussels Summit Declaration[4] at the end of the meeting of the North Atlantic Council in July 2018 stated:

> 'We have agreed a new biometric data policy which, consistent with applicable national and international law and subject to national requirements and restrictions, will further support our ability to identify returning foreign terrorist fighters and other threat actors, and to comply with UNSCR 2396'.

UNSCR 2396/2017 obliges Germany to, *inter alia*, develop a 'system for collecting biometric data [...] with the aim of identifying foreign terrorists'.

---

[1] BVerfG, court decision of May 19th - 1 BvR 2835/17 2020, NVwZ 2020, p.2235 ff.
[2] Notably *Siemsen*, Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten, Schriften zum Öffentlichen Recht, Band 1387, Duncker & Humblot, Berlin, 2018.
[3] S/RES/2396 (2017) – Threats to international peace and security caused by terrorist acts – foreign terrorist fighters.
[4] Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, PR/CP(2018)074, 11th July 2018, para.11.

The question of the extent to which Germany can fulfil its security policy obligations in a multinational environment depends on the possibilities (and limits) for the use of biometric data in connection with international obligations. This question is of practical relevance because, as a member of NATO and the United Nations (UN), Germany's armed forces are engaged both in NATO and UN operations.

## 1.2 Parliamentary inquiries in Germany

The use of biometric data in multinational military operations has been the subject of several parliamentary inquiries[5] in the last years. Most recently, they have concerned the use of the NATO Automated Biometric Identification System (NABIS)[6] which allows for the collection and exchange of biometric data in a multinational military context.[7]

It can be assumed that biometric data is collected in the countries in which NATO operations are carried out[8]. If biometric data is collected in the course of military operations, the question arises, whether (and how) it may be used for the (civil) purposes of hazard prevention or law enforcement[9].

However, from a national point of view, the use of NABIS and law enforcement's use of biometric data collected by the military are only relevant when it has been established, that biometric data collection by the Bundeswehr during deployments abroad is acceptable under current law.

The Federal Government has admitted that German soldiers collected biometric data in Afghanistan as part of the International Security Assistance Force (ISAF).[10] It was stated that biometric data consisting of fingerprints, iris images and 'face geometry' has been collected from Afghan citizens and handed over to U.S. authorities. Mobile devices were afterwards used to identify people by matching the collected biometric data against a U.S. database. This procedure describes a system for biometric authentication, in which biometric characteristics are stored to enable the later identification of an individual. Those three exemplary biometric characteristics are often used for biometric authentication systems due to their reliability.[11] The Federal Government also produced its legal assessment that the collection of biometric data was lawful as it was covered by the ISAF mandate and that in any case, the (since-revised) German Federal Data Protection Act (FDPA)[12] did not apply to foreigners abroad anyway. Applying this argument, it was only logical for the Federal Government not to address data protection law at all.

This is where this paper takes a different approach. Although the ISAF mission is long over[13] and the European legal landscape for data protection was fundamentally changed with the entry into force of

---

[5] These inquiries are brought forward by a parliamentary fraction and address the Federal Government, see section 104 in conjunction with section 75 of the German parliamentary rules of procedures.
[6] Parliamentary publication 19/12556 of August 21st 2019. For an overview of the system, see NATO Automated Biometric Identification System (NABIS) - YouTube.
[7] *Coman/Niculescu*, MTA Review Vol XXVII, No. 2, Dec. 2017, p.67, 69.
[8] NATO establishes biometric database, US military has it already – Matthias Monroy (site36.net).
[9] Law enforcement usage of personal data collected by the military in „theatres of war" was the subject of yet another parliamentary inquiry, see parliamentary publication 19/9641 of April 24th 2019; parliamentary publication 19/10080 of May 10th 2019.
[10] Parliamentary publication 17/6862 of August 26th 2011 in response to Parliamentary publication 17/6744 of August 3rd 2011.
[11] DSK-Positionspapier, p.8 'statische Merkmale' ('static characteristics').
[12] Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097).
[13] The ISAF mission ran from the 20th of December 2001 till the 31st of December 2014. Also the follow-on Resolute Support Mission will conclude in 2021.

the European General Data Protection Regulation (GDPR) [14], the scenario of collecting biometric data during deployment is more relevant than ever[15].

[14] 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), Official Journal of the European Union L 119/1, May 4th 2016.

[15] See with a comprehensive analysis; *Zwanenburg*, Biometrics on the Battlefield, available under; https://lieber.westpoint.edu/biometrics-on-the-battlefield/.

# 2. Legal determinants of the analysis

## 2.1 The applicability of the GDPR

The analysis of national data protection issues begins with a look at secondary EU law. From its title, it is clear that the GDPR was intended to ensure the 'protection of natural persons when processing personal data'. As an EU regulation, the GDPR is directly applicable in all member states - at least insofar as the provisions made in it are final or leave no room for deviations nor require national implementing acts. Within the GDPR there are several opening clauses which give the member states the opportunity to fill in and design intended loopholes by means of national regulations. Therefore the GDPR is correctly described as a hybrid between an EU Regulation within the meaning of Article 288(2) of the Treaty on the Functioning of the European Union (TFEU) and an EU Directive according to Article 288(3) TFEU.[16]

For the member states of the EU, the material scope of the GDPR is determined by Article 2(2)(a), according to which the Regulation does not apply to the processing of personal data concerning activities that do not fall within the scope of Union law. Recital 16 sentence 1 of the GDPR lists national security under that heading and thus refers to Article 4(2) sentence 3 of the Treaty on European Union (TEU) which makes it clear that national security remains the sole responsibility of the individual member states. Although the term 'national security' is not conclusively defined, defence policy decisions will be covered by it.[17]

It goes without saying that the GDPR only applies to the member states of the European Union[18], but should be expressly mentioned again at this point. Because when German (or any other EU member states) armed forces deploy abroad, it usually happens in a multinational context. Especially within NATO mission, we can encounter cooperation between member states of the EU (thus GDPR-bound) as well as third countries (like the U.S., Canada or Turkey). Different data protection standards have the potential to add a certain layer of complexity to this multinational operations.

## 2.2 The scope of the FDPA

Germany transposed the GDPR into national law in 2018[19] through an amendment of the FDPA[20] which is now shaped by the GDPR to such an extent, that national data protection questions can only be answered meaningfully by looking at the two legal instruments together.

It is true that EU regulations are issued with the aim of achieving the greatest possible harmonization of legal provisions throughout the member states of the EU. Nonetheless, via the above mentioned opening clauses of the GDPR, the European legislator laid the foundation for the member states to implement their own ideas about data protection law. Those ideas are often about "more" data protection may be implemented compared to the requirements of the GDPR, even if this runs counter to the harmonizing efforts of the European legislator.

---

[16] *Kühling/Martini*, EuZW 2016, p.448, 449.
[17] *Karpenstein/Sangi*, GSZ 2020, p.162, 167.
[18] Article 1(1) TEU.
[19] The GDPR was applied directly in the member states starting from May 25th, 2018, see Article 99(2) GDPR.
[20] See Articel 8(1) sentence 1 of the Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU.

Also Germany aimed at surpassing the standards of the GDPR.

Regardless of the question of how far the exclusion of Article 2(2)(a) GDPR in conjunction with Article 4 TEU extends in regard to national security, the German legislature had the right to establish a 'full data protection regime' [21] to ensure that there are no areas free of data protection at the national level.

The instrument for establishing this 'full data protection regime' is the provision of Section 1(8) FDPA:

> 'Regulation (EU) 2016/679 and Parts 1 and 2 of this Act shall apply accordingly to processing of personal data by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 unless otherwise provided for in this or another Act'.

Therefore, from a national point of view, the question does not arise whether the processing of biometric data by the armed forces falls under the application exception of Article 2(2)(a) GDPR because this exclusion would be overruled by Section 1(8) FDPA.

Section 1(8) FDPA orders a 'corresponding applicability' for parts 1 and 2 of the FDPA as well as for the provisions of the GDPR. For the fourth part of the FDPA ('Special provisions for processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680') this is not necessary.

Section 85 FDPA regulates the 'processing of personal data in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680'. The subject of this regulation is, among other things, the transmission of data to supranational or intergovernmental organisations or to third countries. Part 4 of the FDPA and in particular Section 85 are the direct consequence of the legislative intention to establish a full data protection regime. In this regard Section 85 FDPA directly supplements Section 1(8) FDPA.[22]

## 2.3 Terminology of the GDPR

When talking about the processing of biometric data, it is important to briefly identify the legal definitions involved. According to Article 4 No. 14 GDPR, biometric data is:

> 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'.

Fingerprints, iris images and face geometry which are mentioned in parliamentary publication 17/5744 are therefore biometric data in the sense of EU secondary law.

From the wording of the definition according to Article 4 No. 14 GDPR, two more things can be deducted. First, it is made clear that 'biometric data' is 'personal data' under the definition of Article 4 No. 1 GDPR:

> 'any information relating to an identified or identifiable natural person'.

Second, it can be concluded from the connection with Article 9 GDPR that the EU intended to include biometric data under the term 'special category of personal data'.[23] The processing of 'special categories of personal data' is prohibited under Article 9(1) GDPR and only permitted in exceptional cases allowed under Article 9(2). This construction is justified with the particular sensitivity of biometric data, the

[21] Parliamentary publication 18/11325, p.96; Taeger/Gabel/*Schmidt* BDSG § 1 Rn. 39.
[22] BeckOK DatenschutzR/*Wolff* BDSG § 85 Rn. 1.
[23] According to recital 10 of the GDPR, the term 'sensitive data' should be used synonymously.

processing of which can result in considerable risks for the fundamental rights and freedoms of the person concerned.[24]

This vulnerability leads to the prominent position assigned to the biometric data in the system of EU data protection law and its need for special protection.[25] The secondary law prohibition[26] relates to the *processing* of biometric data. According to Article 4 No. 2 GDPR, the term 'processing' refers to:

> 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

As can be deducted from the scenario in parliamentary publication 17/6862, German soldiers were entrusted with the collection[27] of biometric data and transmission[28] of biometric data to U.S. authorities. These activities are listed as sub-cases of processing in Article 4 No. 2 GDPR.

## 2.4 The extraterritorial applicability of the FDPA

Concerning the scenario of parliamentary publication 17/6862,[29] the Federal Government argued, that during a deployment, in addition to the international and constitutional requirements national regulations must be observed if they are applicable, but this was not the case with the FDPA.[30] This legal opinion was finally rejected by the Federal Constitutional Court. The court held that:

> 'the binding of the German state authority to the fundamental rights according to Article 1(3) Basic Law is not limited to the German state territory […] the protection of the individual basic rights (can) differ at home and abroad'.

The judgment dealt with the fundamental rights stemming from Article 10(1) (telecommunications secrecy) and Article 5(1) sentence 2 (freedom of the press). The implications for the constitutional right to informational self-determination arising from Article 2(1) in conjunction with Article 1(1) of the Basic Law are discussed below.

In conclusion, the FDPA – as well as the GDPR – is applicable to the German armed forces whiles deployed abroad.

---

[24] In addition to biometric data, the processing of personal data from which the racial and ethnic origin, political opinion, religious or ideological opinion or trade union membership can be deduced, and the processing of genetic data, health data or data on the sex life or sexual orientation of a natural person is prohibited; BeckOK DatenschutzR / Albers / Veit DS-GVO Art. 9 Rn. 15 ff.
[25] See recital 51 of the GDPR; comprehensive on the differences between 'simple' personal data and biometric data; *Matejek/Mäusezahl*, ZD 2019, p.551.
[26] BeckOK DatenschutzR/*Albers/Veit* DS-GVO Art. 9 Rn. 1; Paal/Pauly/*Frenzel* DS-GVO Art. 9 Rn. 1; Taeger/Gabel/*Mester* DS-GVO Art. 9 Rn. 2.
[27] Parliamentary publication 17/6862, p.5.
[28] Parliamentary publication 17/6862, p.7.
[29] Parliamentary publication 17/6744, p.2.
[30] Parliamentary publication 17/6862, p.4.

# 3. The processing of biometric data based on the FDPA

## 3.1 National legal foundation

Section 22 FDPA formulates the national legal basis for the processing of special categories of personal data.[31] The case groups formulated in Section 22(1) No. 1 and No. 2 FDPA are not congruent with the opening clauses in Article 9(2) GDPR.[32] On the question of the processing of biometric data by the Bundeswehr, Section 22(1) No. 2(c) FDPA is decisive:

> 'By derogation from Article 9(1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679 shall be permitted [...] by public bodies if [...] processing is necessary for urgent reasons of defence [...] and as far as the interests of the controller in data processing [...] outweigh the interests of the data subject'[33].

In doing so, the legislature specifically makes use of the opening clause provided for in Article 9(2)(b) GDPR, according to which the secondary law prohibition on the processing of biometric data according to Article 9(1) does not apply if

> 'the processing is necessary for reasons of substantial public interest, on the basis of [...] 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'.

The wording of Article 9(2)(g) GDPR and Section 22(1) No. 2(c) FDPA are not identical; in terms of content, however, the national legal basis does not lag behind European secondary law.[34]

Instead, it even seems to be the case that the 'urgent' reasons in Section 22(1) No. 2(c) FDPA represents a tightening of the requirements from Article 9(2)(g) GDPR. This is permissible under Article 9(4) GDPR, according to which the member states can introduce or maintain additional conditions, including restrictions. However, relief about the permissibility of the processing of biometric data is not covered by Article 9(4) GDPR.[35] Although determined by the GDPR, the national legal basis for the processing of biometric data remain exceptional provisions[36] and are therefore to be interpreted narrowly.

For this paper's subject, from Section 22(1) No. 2(c) FDPA the following admissibility requirements are identified:

- Processing only by public bodies;
- Processing for (urgent) reasons of defence only;

---

[31] Parliamentary publication 18/11325, p.70; BeckOK DatenschutzR/*Albers/Veit* BDSG § 22 Rn. 9; Gola/Heckmann/*Heckmann/Scheurer* BDSG § 22 Rn. 1.
[32] A helpful overview can be found at Taeger/Gabel/*Rose* BDSG § 22 Rn. 5.
[33] Besides for „urgent reasons of defence", Section 22(1) No. 2(c) FDPA also permits the processing of biometric data also for the fulfilment of supra- or intergovernmental obligations of a public body of the Federation in the field of crisis and the management or conflict prevention or for humanitarian measures. Both of these alternatives bear no relevance for this paper.
[34] Taeger/Gabel/*Rose* BDSG § 22 Rn. 6.
[35] Gola DS-GVO/*Schulz* DS-GVO Art. 9 Rn. 48; Ehmann/Selmayr/*Schiff* DS-GVO Art. 9 Rn. 64; dissenting opinion Kühling/Buchner/*Weichert* DS-GVO Art. 9 Rn. 150 with further annotation.
[36] Parliamentary publication 18/11325, p.94.

- Processing only if this is necessary; and
- Processing only after a weighing of interests.

## 3.2 Public bodies

Section 22(1) No. 2(c) FDPA only authorizes 'public bodies' to process biometric data for reasons of defence. According to the definition in Section 2(1) FDPA, public bodies at the federal level are:

> 'the authorities, judicial bodies and other public law institutions of the Federation, of direct federal corporations, statutory bodies and foundations established under public law and of their associations irrespective of their legal form'.

As can be seen from the clause 'and other institutions organised under public law', the term is intended to cover any state action regardless of the form of organisation.[37] There can be no doubt that the military and the civilian parts of the Bundeswehr[38] fall under this concept of public bodies. In parliamentary publication 17/6862, the Federal Government assumed that, in principle, every person in a German contingent would be authorized to record biometric data and that there would be no restriction in terms of rank or branch of service.[39]

According to Section 2(4) sentence 2 FDPA, a non-public body[40] is also considered a public body within the meaning of this Act, insofar as it performs public administration tasks. This would allow the transfer of the processing of biometric data to private companies.

## 3.3 Data processing for reasons of defence

The processing of biometric data may only take place if it is necessary for (urgent) reasons of defence, yet this term is not defined in Section 22(1) No. 2(a) FDPA, and neither does the explanatory memorandum for the FDPA give any indication about it. The same applies to the opening clause of Article 9(2) (g) GDPR, which only refers to a 'significant public interest' without specifying this in more detail.[41]

The term 'defence' does appear in the GDPR as a distinction to the term 'national security'. For example, Article 23(1) authorises member states to restrict the rights and obligations from Chapter III of the GDPR for reasons of national security ((a) but also national defence (b)).[42] Elsewhere, the GDPR only speaks of 'defence'.[43]

---

[37] Kühling/Buchner/*Klar/Kühling* BDSG § 2 Rn. 9; BeckOK DatenschutzR/*Schild* § 2 Rn. 8.
[38] The term Bundeswehr includes both the (military) armed forces and the (civil) federal defence administration; Maunz/Dürig/*Depenheuer* GG Art. 87a Rn. 70.
[39] Parliamentary publication 17/6862, p.5.
[40] Private bodies are natural and legal persons, societies and other associations established under private law unless they are covered by subsections 1 to 3, section 2(4) sentence 1 FDPA.
[41] Ehmann/Selmayr/*Schiff* DS-GVO Art. 9 Rn. 51 points out that the scope of this opening clause is most likely to be found in public security law or in law to prevent danger, but also makes it clear that the 'significant public interest' is not limited to a specific legal matter; likewise, Taeger/Gabel/*Mester* DS-GVO Art. 9 Rn. 28.
[42] Ehmann/Selmayr/*Bertermann* DS-GVO Art. 23 Rn. 3 assumes that the terms 'national security' and 'national defence' describe (probably national) external security (in particular, to differentiate it from the internal security of a member state, Article 23(1) GDPR uses the term 'public security').
[43] Article 45(2)(a) GDPR.

Given that the opening clause is intended to be filled with national legislation, it seems only logical to consider the concept of defence in Section 22(1) No. 2(a) FDPA through a national lens. Taking into account the principle of the integrity of the legal order, this speaks in favour of understanding the term 'defence' as it is understood by the German constitution. Article 87a(1) sentence 1, (2) of the Basic Law is the central norm, according to which the Federation sets up armed forces for defence. The constitutional concept of defence is mostly understood in the literature as 'broad',[44] and also as 'open to development'.[45] In recent years, the view that Article 87a(1) sentence 1 of the Basic Law also incorporates collective defence according to Article 5 of the North Atlantic Treaty and Article 51 of the UN Charter seems to have prevailed.[46]

The Bundeswehr is currently engaged in 12 different military deployments with around 3,500 personnel on 3 different continents.[47] Even if the classic notion of national defence is coming back into focus in the current strategic environment[48], it seems that the operational focus of the Bundeswehr will continue to be within the framework and according to the rules of collective multinational security systems and outside of German territory.

If one also encompasses the engagement of the German armed forces in an authorised foreign deployment under the concept of 'defence' within the meaning of Article 87a of the Basic Law, then the entire range of military tasks required to carry out the mandate must also be included, thus covering any lawful act by German personnel. This comprises not only when biometric data is used to implement access control[49] and thus improve the protection of personnel. The use of biometric data for military operations management and generally to improve the security situation in the operational area would also be covered.[50]

In this context, it is also instructive to take a look at the explanatory memorandum of the FDPA, which states that there must be a 'significant public interest' to meet the requirements of the legal basis of Section 22(1) No. 2(a) FDPA:

> 'in particular in cases where biometric data are processed for the purpose of clearly identifying those affected'.[51]

Section 22(1) No. 2(a) FDPA permits the processing of biometric data by public bodies if it is necessary to avert a significant danger to public safety.

Since the 'significant public interest' as a formulation has not found its way into Section 22(1) No. 2(a) FDPA, it can be assumed that this is an editorial mistake in the explanatory memorandum because there actually is a reference to the national interpretation of the 'significant public interest' within the meaning of Article 9(2)(g) GDPR. In any case, it would be arbitrary to apply this reasoning only to Section 22(1) No. 2(a) FDPA, which should be relevant in the field of internal security, and not also to Section 22(1) No. 2(c) FDPA.

---

[44] Jarass/Pieroth GG Art. 87a Rn. 10.
[45] BeckOK GG/*Epping* GG Art. 87a Rn. 4.
[46] Jarass/Pieroth GG Art. 87a Rn. 11; v. Münch/Kunig/*Aust* GG Art. 87a Rn. 35 with reference to the principle of the Basic Law's friendliness towards international law; in summary v. Mangoldt/Klein/Starck/*Müller-Franken* GG Art. 87a Rn. 39; *Wiefelspütz*, ZaöRV 2005, p.819, 823.
[47] See https://www.bundeswehr.de/de/einsaetze-bundeswehr.
[48] Positionspapier: Gedanken zur Bundeswehr der Zukunft, p.5.
[49] Parliamentary publication 17/6862, p.3.
[50] Parliamentary publication 17/6862, p.4.
[51] Parliamentary publication 18/11325, p.95.

## 3.4 Necessity of processing

Both the opening clause of Article 9(2)(g) GDPR and Section 22(1) No. 2(c) FDPA raise the question of the necessity of data processing. Necessity implies that the state must use the mildest available means of equal effectiveness to achieve a goal.[52] The Bundeswehr's foreign missions regularly take place in countries whose state structures cannot be compared with those in Europe and whose security situation must be described as fragile. The reason given for the biometric enrolment of Afghans was that it would lead to an 'improved possibility of access control to ISAF properties'.[53] This means determining identity by comparing biometric data with information that has already been stored in a database.[54] This scenario also played an essential role in the development of Section 22 of the FDPA. When it comes to the question of alternative milder options to increase the security of personnel, the control of identification documents should be considered. Yet identity documents can be forged much more easily than biometric characteristics and so to achieve the legislative goal of safeguarding German personnel, the control of identity documents would have to be as fraud-resistant as biometric identification.[55]

Under Section 22(1) No. 2(c) FDPA, however, the necessity test is specified by the 'urgency' feature. While the 'reasons of defence' refer to the occasion or the environment of the data processing, the adjective 'urgent leads to an increase in the requirements for the admissibility of the data processing at the level of the necessity test. Accordingly, data processing based on Section 22(1) No. 2(c) FDPA must always be of 'urgent necessity'.[56]

## 3.5 Weighing and securing of interests

For any data processing based on Section 22(2) No. 2 FDPA, a predominance of the interests of the person responsible for the data processing over the interests of the person concerned is necessary as a precondition for admissibility.[57] This admissibility requirement necessitates a process in which the conflicting[58] positions are identified and their value considered. Biometric data is categorised under European law as sensitive and placed under special protection.[59] The GDPR states in Article 9(2)(g) that in particular the 'essence of the right to data protection'[60] and the 'fundamental rights of the data subject' must be considered. These aspects are to be included in the assessment, even if they are not explicitly repeated in the wording of Section 22(1) No. 2(c) FDPA; Section 22(2) FDPA has to be regarded as sufficient.[61]

---

[52] Sachs/*Sachs* GG Art. 20 Rn. 152 with comprehensive evidence of case law; also, Maunz/Dürig/*Grzeszick* GG Art. 20 Rn. 113 which postulates the principle of choosing the mildest remedy.
[53] Parliamentary publication 17/6862, p.3.
[54] See the introduction to the technical basics of biometric authentication by the BSI and section 5.2 of the position paper on the biometric analysis of the DSK.
[55] See *Mitchell*, The Canadian Yearbook of International Law 2012, p.289, 296/297, also referring to *Shanker*, New York Times 31. July 2011, in the same sense *Lunan*, The Three Swords Magazine 2018, p.37, 38, as well as the United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counterterrorism, p.13.
[56] Which is why 'high demands are placed on the realization of the facts' in the commentary literature, see BeckOK DatenschutzR/*Albers/Veit* BDSG § 22 Rn. 22.
[57] BeckOK DatenschutzR/*Albers*/*Veit* § 22 Rn. 23.
[58] 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; [...], see Article 4 No. 7 GDPR.
[59] BeckOK DatenschutzR/*Albers*/*Veit* § 22 Rn. 23; Paal/Frenzen/*Pauly* BDSG § 22 Rn. 11.
[60] For the term see Ehmann/Selmayr/*Schiff* DS-GVO Art. 9 Rn. 55 with further annotations
[61] Taeger/Gabel/*Rose* BDSG § 22 Rn. 7 referring to parliamentary publication 18/11325, p.95.

The constitutional right to informational self-determination derived from Articles 1(1) and 2(1) of the Basic Law protects the individual against the collection and processing of personal data by the state. This fundamental right[62] applies also to non-German nationals. It is also clear that the highest German court attaches particular importance to European legal acts.[63] Article 8(1) of the Charter of Fundamental Rights of the European Union has to be considered also.[64] If the Federal Intelligence Service is 'constrained by the rule of law' [65] by the Court's ruling concerning its foreign activities, no other standard can be applied to the Bundeswehr.

However, as the processing of biometric data by the Bundeswehr on foreign deployments is also carried out to increase their own security, it seems justifiable under Section 22(1) No. 2(c) FDPA that the balance of interests would favour the admissibility of biometric data processing, particularly if the instruments provided in Section 22(2) FDPA are used and appropriate and specific measures are taken to safeguard the interests of the person concerned. These are:

- measures to increase awareness of staff involved in processing operations (Section 22(2) sentence 2 No. 3 FDPA);
- restrictions on access to personal data within the controller and by processors (Section 22(2) sentence 2 No. 5 FDPA); and
- the encryption of personal data (Section 22(2) sentence 2 No. 7 FDPA).

A look at the scenario shows that various measures have been taken which are likely to affect the balance of interests. The Federal Government has explained that the personnel who are used to collect biometric data have not only been instructed in the operation of the devices themselves, but also in terms of issues of data protection and the protection of fundamental rights.[66] Officers have been appointed within the German contingent to check compliance with the law before forwarding the data.[67] Finally, it seems to have been stipulated that the data collected by German ISAF forces cannot be used or passed on for purposes other than those of ISAF without the consent of the Bundeswehr.[68]

[62] See BVerfGE 65, 1 („Volkszählungsurteil'). An overview of this v. Münch/Kunig/*Kunig/Kämmerer* GG Art. 2 Rn. 75 ff.
[63] See BVerfG, court decision of May 19th, 2020, para. 96.
[64] Article 8(1); 'Everyone has the right to the protection of personal data concerning him or her', see Charter of Fundamental Rights of the European Union (2012 / C 326/02); Official Journal of the European Union of October 26, 2012, C 326/391.
[65] Using this formulation *Aust*, DÖV 2020, p.715 ff.
[66] Parliamentary publication 17/6862, p.6.
[67] Parliamentary publication 17/6862, p.7.
[68] Parliamentary publication 17/6862, p.8.

# 4. Concluding remarks

Although biometric data is particularly sensitive at both European and national levels and must be protected accordingly, processing by the Bundeswehr during deployment abroad is lawful. Due to the decision of the German legislature on the application order of Section 1(8) FDPA to establish a 'full data protection regime' for state action, the processing operations are based not only on national data protection law but also indirectly on the GDPR. Parliamentary publication 17/6744 listed which elements are to be observed within the framework of the regulations and which legal interests have to be weighed. It is clear that, at least in deployment areas in which Bundeswehr personnel are exposed to high risk, the processing of biometric data by the Bundeswehr for access control may in general be permissible.

With reference to the aforementioned *UNSCR 2396/2017* as well as the *Brussels Summit Declaration*, the processing of biometric data in the context of multilateral military operations is likely to become more common. In particular, the use of NABIS raises questions about exchanging special categories of personal data with and within international organisations.

Given the many unresolved legal questions in this area, it would be desirable for this topic to be investigated further. Because in the end, it will be the answer as to what is legally possible which will decided whether or not an emerging technology can be employed successfully in multinational military missions.

# Bibliography


**Legal acts**

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)

Bundesdatenschutzgesetz (Federal Data Protection Act – FDPA)

Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)

Grundgesetz für die Bundesrepublik Deutschland (Basic Law)

Fundamental Rights of the European Union (2012 / C 326/02); Official Journal of the European Union of October 26, 2012, C 326/391

**Articles**

*Aust, Helmut Phillip*, 'Auslandsaufklärung durch den Bundesnachrichtendienst: rechtsstaatliche Einhegung und grundrechtliche Bindungen im Lichte des Urteils des Bundesverfassungsgerichts zum BND-Gesetz', Die Öffentliche Verwaltung (DÖV) 2020, p.715-724

*Niculescu, Bogdan R. / Coman, Cristian*, 'NATO Automated Biometric Identification System (NABIS)', MTA Review Vol XXVII, No. 2, Dec. 2017, p.67-72

*Karpenstein, Ulrich / Sangi, Roya*, 'Nationale Sicherheit im Unionsrecht: Zur Bedeutung von Art. 4 II 3 EUV', Zeitschrift für das Gesammte Sicherheitsrecht (GSZ) 2020, p.162-168

*Kühling, Jürgen / Martini, Mario*, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?', Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2016, p.448-454

*Lunan, Mark*, 'New Doctrinal Concepts Biometrics', The Three Swords Magazine 2018, p.37-41

*Matejek, Michaela / Mäusezahl, Steffen*, 'Gewöhnliche vs. Sensible personenbezogene Daten – Abgrenzung und Verarbeitungsrahmen von Daten gem. Art. 9 DS-GVO', Zeitschrift für Datenschutz (ZD) 2019, p.551-556

*Mitchell, Alison*, 'Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics', The Canadian Yearbook of International Law 2012, p.289-330

*Wiefelspütz, Dieter*, 'Der Auslandseinsatz der Bundeswehr gegen den grenzüberschreitenden internationalen Terrorismus', Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV) 2005, p.819-835

**Commentaries**

*Brink, Stefan / Wolff, Heinrich Amadeus*, 'BeckOK Datenschutzrecht', 35. Auflage 2021, C.H.BECK, München

*Ehmann, Eugen / Selmayr, Martin*, 'Beck'sche Kurz-Kommentare DS-GVO Datenschutz-Grundverordnung', 2. Auflage 2018, C.H.BECK, München

*Epping, Volker / Hilgruber, Christian*, 'BeckOK Grundgesetz', 46. Edition 2021, C.H.BECK, München

*Gola, Peter / Heckmann, Dirk*, 'Bundesdatenschutzgesetz', 13. Auflage 2019, C.H.BECK, München

*Jarass, Hans D. / Pieroth, Bodo*, 'Grundgesetz für die Bundesrepublik Deutschland', 16. Auflage 2020, C.H.BECK, München

*Kühling, Jürgen / Buchner, Benedikt*, 'Datenschutz-Grundverordnung BDSG Kommentar', 3. Auflage 2020, C.H.BECK, München

*Mangoldt, Herman von/ Klein, Friedrich / Starck, Christian*, 'Grundgesetz', 7. Auflage 2018, C.H.BECK, München

*Maunz, Theodor / Dürig, Günter*, 'Grundgesetz Kommentar', 93. Lieferung, Oktober 2020, C.H.BECK, München

*Münch, Ingo von / Kunig, Philip*, 'Grundgesetz', 7. Auflage 2021, C.H.BECK, München

*Paal, Boris P. / Pauly, Daniel A.*, 'Beck'sche Kompakt-Kommentare Datenschutzgrundverordnung Bundesdatenschutzgesetze', 3. Auflage 2021, C.H.BECK, München

*Taeger, Jürgen / Gabel, Detlev*, 'Kommentar DSGVO – BDSG', 3. Auflage 2019, Fachmedien Recht und Wirtschaft, dfv Mediengruppe, Frankfurt am Main

*Sachs, Michael*, 'Grundgesetz', 9. Auflage 2021, C.H.BECK, München

**Other**

Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, PR/CP(2018)074, July 11th 2018

Bundesamt für Sicherheit in der Informationstechnik: Einführung in die technischen Grundlagen der biometrischen Authentisierung, available under: Einführung in die technischen Grundlagen der biometrischen Authentisierung (bund.de)

Bundestagsdrucksache (Parliamentary publication) 19/12556 of August 21st 2019

Bundestagsdrucksache (Parliamentary publication) 19/9641 of April 24th 2019

Bundestagsdrucksache (Parliamentary publication) 19/10080 of May 10th 2019

Bundestagsdrucksache (Parliamentary publication) 17/6862 of August 26th 2011

Bundestagsdrucksache (Parliamentary publication) 17/6744 of August 3rd 2011

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Positionspapier zur biometrischen Analyse, Version 1.0, Stand: 3. April 2019 (DSK-Positionspapier)

*Monroy, Matthias*, 'NATO establishes biometric database, US military has it already', November 8th 2019, available under: NATO establishes biometric database, US military has it already – Matthias Monroy (site36.net)

Positionspapier: Gedanken zur Bundeswehr der Zukunft, Bundesministerium der Verteidigung – Die Bundesministerin / Der Generalinspekteur, Berlin, February 9th 2021

Security Council Resolution (S/RES) 2396 (2017) – Threats to international peace and security caused by terrorist acts – foreign terrorist fighters

*Shanker, Thom*, 'To track Militants, U.S. has System that never forgets a face', New York Times, July 31th 2011

*Siemsen, Annelie*, Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten, Schriften zum Öffentlichen Recht, Band 1387, Duncker & Humblot, Berlin, 2018

United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, compiled by CTED and UNOCT, 2018

*Zwanenburg, Marten*, Biometrics on the Battlefield, October 21th 2020, available under: Biometrics on the Battlefield | Lieber Institute West Point.