Schlussbericht und Empfehlungen

vom 17. Juni 2022

mit Ergänzungen vom 13. Oktober 2022

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
(EDÖB)

im Verfahren gemäss
Artikel 29 des Bundesgesetzes vom 19. Juni 1992
über den Datenschutz (DSG; SR 235.1)

betreffend das von der
Stiftung Swisstransplant mit Sitz in Bern betriebene

Nationale Organspenderegister (NOSR)

Inhalt

1. Einführung

1.1. Zuständigkeit und Kontext

1 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) klärt von sich aus oder auf Meldung Dritter hin einen Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (sog. Systemfehler). Gemäss Art. 29 Abs. 2 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) kann er dabei Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen.

2 Swisstransplant (nachfolgend «SWT») ist eine privatrechtliche Stiftung. Im Auftrag des BAG ist sie die nationale Zuteilungsstelle im Sinne des Art. 19 des Bundesgesetzes über die Transplantation von Organen, Geweben und Zellen (Transplantationsgesetz; SR 810.21). In dieser Funktion führt sie insbesondere die Warteliste der Personen, die auf eine Organtransplantation warten, und verwaltet die Zuteilung der Organe. Parallel zu diesen Aktivitäten hat sie das «Nationale Register für Organspenden» (Nationales Organspenderegister, nachfolgend «NOSR») entwickelt. Dabei handelt es sich um ein elektronisches Register, in dem eine Person ihren Willen zur Organ- und Gewebespende für den Fall ihres Todes festhalten kann

3 Am 11. Januar 2022 wurde der EDÖB von einem Journalisten kontaktiert, der ihm einen Bericht der deutschen IT-Sicherheitsfirma ZFT.GmbH (Ergebnisreport Untersuchung «Nationales Organspenderegister» vom 10.01.2022, nachfolgend «Bericht ZFT») vorlegte. Der Bericht zeigte mehrere Mängel im NOSR auf, insbesondere in Bezug auf die Sicherheit der Registrierungsprozesse.

4 Bis dahin gab es drei Registrierungswege für das NOSR: Eintragung per Computer, auf dem Postweg, sowie per Smartphone oder Tablet (vgl. Ziff. 2.3.2 und 2.3.3). Bei der letztgenannten Methode beruhte die Identifizierung des Nutzers im Wesentlichen in der Aufnahme eines Selbstportraits (Selfies). Der ZFT.GmbH gelang es, mittels dieses Prozesses einen Eintrag für eine Drittperson zu fingieren, ohne dass die betreffende Person mitwirken musste. Dieser Vorgang wurde im Rahmen der journalistischen Aufbereitung des Berichts dokumentiert. Anstelle eines Selfies verwendete die ZFT.GmbH ein im Internet gefundenes Foto der Person (in diesem Fall des Journalisten).

5 Es war also mit grundlegenden Computerkenntnissen und wenig technischen Mitteln möglich, eine Person ohne ihr Wissen in das NOSR einzutragen. Andere Registrierungsmethoden wurden in dem

Bericht von ZFT nicht thematisiert. Es sei jedoch vorweggenommen, dass bei keiner dieser Methoden eine amtliche Überprüfung der Identität vorgenommen wurde. Bei der Variante «Postweg» wurde die Postadresse als Identifikationsmittel verwendet, bei der Eintragung über den Computer wurde die Kopie eines Identitätsnachweises verlangt.

6 Nach einer summarischen Plausibilisierung der im Bericht ZFT beschriebenen Mängel eröffnete der EDÖB am 13. Januar 2022 eine Sachverhaltsabklärung.

1.2. Partei und Beteiligte

7 Das Nationale Organspenderegister NOSR wird von der Stiftung Swisstransplant mit Sitz in Bern (CHE-100.390.782) betrieben. Für die Stiftung handelten im vorliegenden Verfahren [redacted], Medical Director / CEO und [redacted], Chief Administrative Officer.

8 Das vorliegende Verfahren wurde von folgenden Mitarbeitenden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) instruiert:

Nathalie Weber, Leiterin Team 1 Direktionsbereich Datenschutz

Joël de Montmollin, Jurist Team 1 Direktionsbereich Datenschutz

Philippe Schwab Molnar, Informations- und Sicherheitsspezialist Kompetenzzentrum IT und digitale Gesellschaft

Marc-Olivier Tricot, Informations- und Sicherheitsspezialist Kompetenzzentrum IT und digitale Gesellschaft

9 Weitere Beteiligte im Verfahren sind die Begasoft AG mit Sitz im Bern, Informatikdienstleisterin für den Betrieb des NOSR, und die [redacted] AG, mit Sitz in [redacted] Anbieterin eines Identifikationstools.

1.3. Umfang der vorliegenden Sachverhaltsabklärung

10 Die vorliegende Sachverhaltsabklärung hat zum Ziel, die im Zusammenhang mit einer journalistischen Recherche bekannt gewordenen Mängel des NOSR in Bezug auf die Datenschutzkonformität und die Datensicherheit insbesondere hinsichtlich der Identifikation im Moment der Eintragung in das Register zu untersuchen. Wie der Beauftragte in seiner Medienmitteilung vom 18. Januar 2021 festgestellt hatte, war die Bekanntmachung der angezeigten Mängel geeignet, das Vertrauen der

Öffentlichkeit in das System der Organspende in der Schweiz zu beeinträchtigen. Vor diesem Hintergrund soll die eingeleitete Sachverhaltsabklärung auch dazu beitragen, dass trotz Fehlens einer staatlich anerkannten elektronischen Identität datenschutzkonforme Lösungen zur Bearbeitung der fraglichen Personendaten gefunden werden können.

11 Im Wesentlichen werden die verschiedenen bisherigen und zukünftigen Registrierungsprozesse – also alle Schritte bis zur Bestätigung einer Registrierung durch SWT – auf ihre Datenschutzkonformität hin untersucht. Auch der Zugriff auf ein bestehendes Konto und die Änderungsmöglichkeiten werden besprochen.

12 Hingegen handelt es sich bei der vorliegenden Sachverhaltsabklärung nicht um eine umfassende organisatorische und technische Prüfung des NOSR, auch wenn nachfolgend einige grundlegende IT-Aspekte thematisiert werden. Es handelt sich auch nicht um eine umfassende Überprüfung der Stiftung SWT selbst und ihrer anderen Aktivitäten oder gar des gesamten Organspendesystems in der Schweiz.

13 Die ZFT.GmbH hat in ihrem Bericht auch eine Lücke bezüglich einer im Zusammenhang mit Lebertransplantationen genutzten Anwendung aufgedeckt, die es Unbefugten hätte ermöglichen können, Patientendaten einzusehen. Laut SWT sollte die Anwendung Ärztinnen und Ärzten die Möglichkeit geben, potenzielle Spenderinnen und Spender zu bewerten.

14 Diese Applikation war im Februar 2020 eingeführt und im November 2021 deaktiviert und durch ein anderes Produkt ersetzt worden. Anfang 2022 wurden die Anwendung und ihre Datenbank vollständig gelöscht. Die Daten, auf die über die Sicherheitslücke zugegriffen werden konnte, waren nur in pseudonymisierter Form einsehbar.

15 In Anbetracht dessen wurden keine weiteren Untersuchungen zu diesem Thema durchgeführt und auf die Anwendung für Lebertransplantationen wird im vorliegenden Schlussbericht nicht näher eingegangen.

1.4. Chronologie

11.01.2022 Meldung eines Journalisten des Schweizer Fernsehens SRF an den EDÖB über Sicherheitslücken beim NOSR, insbesondere in Bezug auf den Registrierungsprozess.

12.01.2022 Kontaktaufnahme durch den EDÖB mit SWT; regelmässige Kontakte mit der Stiftung während der nächsten zehn Tage (Telefone und E-Mails).

Offline-Schaltung des Registers durch SWT, um die Situation zu beurteilen.

13.01.2022 Eröffnung des Verfahrens nach Art. 29 DSG bezüglich NOSR.

18.01.2022 SWT stellt das Register wieder online, die Registrierungsmöglichkeiten per Smartphone/Tablet und per Post werden jedoch ausgesetzt.

Ausstrahlung der Sendung Kassensturz (SRF 1), mit Präsentation der Schlussfolgerungen des Berichts ZFT, Anwesenheit von [redacted] in der Sendung und Interview mit dem Eidgenössischen Datenschutzbeauftragten Adrian Lobsiger.

21.01.2022 SWT sperrt alle Möglichkeiten, sich in das Register einzutragen, sowie alle Möglichkeiten, Profile zu bearbeiten; nur die Einsichtnahme und das Löschen von Profilen ist für die betroffene Person noch möglich. Das Register steht weiterhin für Anfragen für potenzielle Spenden zur Verfügung.

Registrierungen werden erst wieder mit Zustimmung des EDÖB möglich sein.

27.01.2022 bis 04.04.2022 Doppelter Schriftwechsel zwischen dem EDÖB und SWT, d. h. Fragebogen des EDÖB vom 27. Januar und Antworten von SWT vom 18. Februar, dann Zusatzfragen vom 21. März und Antworten vom 4. April.

12.05.2022 Präsentation des neuen Registrierungsverfahrens über [redacted] in den Räumlichkeiten von SWT. Anwesend waren die Vertreter des EDÖB, der Stiftung SWT, der Begasoft AG und der [redacted] AG. Es folgten mehrere Telefonate und E-Mails zwischen dem EDÖB und SWT.

15.05.2022 Eidgenössische Volksabstimmung: Zustimmung zur "mutmasslichen Einwilligung" bei der Organspende.

1.5. Grundlagen der Sachverhaltsabklärung

16 Der EDÖB stützte sich im Rahmen seiner Sachverhaltsabklärung im Wesentlichen auf folgende Quellen:

- Korrespondenz mit SWT ab Januar 2022, insb. die schriftlichen Eingaben vom 13. Januar, 18. Februar und 4. April 2022 mit Beilagen;
- Bericht der ZFT.GmbH vom 10. Januar 2022;
- öffentlich verfügbare Informationen, insbesondere auf der Webseite www.swisstransplant.org;

- von den Parteien und weiteren Beteiligten mündlich erhaltene Informationen, insbesondere anlässlich der Sitzung vom 12. Mai 2022 mit Vertretern von Swisstransplant, Begasoft AG und [redacted] AG.

17 Schliesslich wird darauf hingewiesen, dass der EDÖB nicht direkt auf die Infrastruktur des NOSR zugegriffen hat.

1.6. Rechtsgrundlagen des Organspenderegisters

18 Nach geltendem Recht darf ein menschliches Organ nur dann entnommen werden, wenn eine ausdrückliche Einwilligung des Spenders bzw. der Spenderin vorliegt. Art. 8 Transplantationsgesetz nennt die Voraussetzungen, die erfüllt sein müssen, damit von einer solchen Einwilligung ausgegangen werden kann. In erster Linie ist auf etwaige Dokumente zu verweisen, die der Patient oder die Patientin hinterlassen hat und in denen er sein, bzw. sie ihr Einverständnis mit der Organentnahme oder seine Ablehnung zum Ausdruck bringt. Ist kein Dokument vorhanden, werden die Angehörigen gefragt, ob ihnen eine Erklärung des Patienten bekannt ist. Letztendlich müssen die Angehörigen über die Entnahme entscheiden und dabei den mutmasslichen Willen des Patienten respektieren. Wenn keine Angehörigen erreicht werden können, wird auf die Entnahme verzichtet. In diesem Zusammenhang ist zu beachten, dass gemäss den Richtlinien der SAMW die vorbereitenden medizinischen Massnahmen nach der Feststellung des Todes auf maximal 72 Stunden begrenzt sind. Den Beteiligten bleibt daher nur wenig Zeit, um über eine Organentnahme zu entscheiden.

19 In Bezug auf die Form der Willensäusserung des potentiellen Spenders gibt das Gesetz keine Vorgaben. Es herrscht also Formfreiheit und jedes Dokument ist an sich zulässig, ob es sich nun um einen Spenderausweis, eine Patientenverfügung, einen Brief oder anderes handelt. In diesem Kontext wurde die NOSR eingeführt: ein Eintrag im NOSR ist dazu bestimmt, als Willensbekundung im Sinne der einschlägigen Bestimmungen des Transplantationsgesetzes berücksichtigt zu werden.

20 Mit Volksabstimmung vom 15. Mai 2022 wurde eine Revision des Transplantationsgesetzes angenommen, die nunmehr das System der mutmasslichen Einwilligung vorsieht.[1] Wenn der Patient keine gegenteiligen Angaben hinterlässt, wird davon ausgegangen, dass er der Organentnahme zustimmt – vorbehaltlich eines Widerspruchsrechts der Angehörigen. In diesem Zusammenhang

[1] https://www.bag.admin.ch/bag/de/home/medizin-und-forschung/transplantationsmedizin/rechtsetzungsprojekte-in-der-transplantationsmedizin/indirekter-gegenvorschlag-organspende-initiative.html

wird vom BAG ein Register eingerichtet, das von der Nationalen Zuteilungsstelle (derzeit SWT) betrieben werden wird (nArt. 10a Abs. 1 Transplantationsgesetz). Wie derzeit im NOSR wird es möglich sein, in diesem Register den Willen zur Spende festzuhalten, d.h. eine Zustimmung, eine Ablehnung oder andere diesbezügliche Erklärungen.

21 Wann diese Revision in Kraft tritt und auf welches Datum das neue Register in Betrieb genommen wird, ist noch nicht bekannt. Gemäss Mitteilung könne die neue Regelung frühestens 2024 eingeführt werden. Es wird klargestellt, dass die Einführung des neuen Registers nicht dazu führt, dass Willenserklärungen, die auf andere Weise abgegeben wurden, ungültig werden – das neue Gesetz verhindert mit anderen Worten nicht die Fortsetzung anderer, heute gültiger Lösungen.

1.7. Zukunft des Registers

22 SWT erklärte, grundsätzlich daran interessiert zu sein, den Betrieb des NOSR fortzusetzen. Dieser Punkt müsse jedoch noch vom Stiftungsrat entschieden werden, was gemäss SWT nach der Veröffentlichung des vorliegenden Berichts erfolgen werde. Die Nutzung des NOSR nach der Einführung des künftigen eidgenössischen Registers sei noch nicht geklärt. Dasselbe gelte für die mögliche Beziehung zwischen dem NOSR und dem neuen Register.

2. Sachverhalt

2.1. Allgemeines zu Swisstransplant und zum Organspenderegister

23 Wie oben bereits dargelegt, ist SWT die Nationale Zuteilungsstelle im Auftrag des Bundesamtes für Gesundheit BAG (Art. 19 Transplantationsgesetz) und nimmt damit die entsprechenden Aufgaben wahr, die das Transplantationsgesetz vorsieht. Dazu gehören insbesondere die Führung der Warteliste der Anwärter auf eine Organtransplantation und die Zuteilung der verfügbaren Organe. Im Auftrag der Schweizerischen Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK) koordiniert SWT auch die Aufgaben, die den Kantonen durch das Transplantationsgesetz zugewiesen werden. Schliesslich nimmt sie im Auftrag des Schweizerischen Verbandes für Gemeinschaftsaufgaben der Krankenversicherer (SVK) und des nationalen Spitalverbandes H+ auch ein Mandat im Zusammenhang mit der Kostenermittlung und der Finanzierung von Transplantationen sowie mit logistischen Aspekten wahr.

24 Das NOSR wurde gemäss SWT auf eigene Initiative der Stiftung aufgebaut. Der Betrieb des Registers sei mit anderen Worten nicht explizit im Mandat des BAG enthalten. Das Register ist seit Oktober 2018 in Betrieb. Laut SWT wird es ausschliesslich aus Mitteln der Stiftung finanziert und nicht durch öffentliche Gelder unterstützt.

25 Beim NOSR handelt es sich um ein elektronisches Register, in dem Einzelpersonen ihren Willen zur Organ- und Gewebespende im Falle ihres Todes festhalten können (Zustimmung oder Ablehnung, ggf. betreffend welcher Organe). Das Ziel des NOSR ist es, eine zentrale, zuverlässige und dauerhafte Datenbank anzubieten, damit der Wille des Verstorbenen besser berücksichtigt werden kann. Es ist dazu bestimmt, von Spitälern systematisch verwendet zu werden.

26 Mit dem NOSR sollte insbesondere zwei Schwierigkeiten im Organspendewesen begegnet werden: zum einen die Tatsache, dass der Spendewille oftmals nicht bekannt ist, zum andern, dass Spenderausweise nicht auffindbar, verloren oder unleserlich sein können.

27 In einer potenziellen Spendesituation – d.h. bei einer Hirntoddiagnose oder der Entscheidung, die Behandlung abzubrechen – kontaktiert die zuständige Person des behandelnden Spitals das NOSR, um in Erfahrung zu bringen, ob der Patient dort registriert ist (vgl. unten Ziff. 2.5). Wenn dies der Fall ist, übermittelt das NOSR dem Spital das Datenblatt, das den Willen des Patienten enthält. Das Dokument hat die Funktion, den Willen des Patienten bekannt zu machen und zu dessen Umsetzung zu verhelfen. Gleichzeitig soll es die Angehörigen entlasten, indem sie einen Hinweis auf den Willen des Verstorbenen erhalten, und erleichtert die Arbeit des Spitalpersonals, wenn diese Problematik mit den Angehörigen besprochen wird.

2.2. Beurteilung der Risiken durch SWT

28 SWT erklärte gegenüber dem EDÖB im Laufe des vorliegenden Verfahrens, dass die bisherigen Registrierungsprozesse, welche nachfolgend (Ziff. 2.3) beschrieben werden, das Risiko unberechtigter Eintragungen in das Register nicht ausschliessen. Sie wies jedoch darauf hin, dass es kein Motiv für mutwillige Falscheinträge gebe. Der Täter könne vernünftigerweise nicht davon ausgehen, dass er einen persönlichen Vorteil daraus zieht, da die Fälle tatsächlicher Spenden selten seien. SWT wies darauf hin, dass auch bei Spenderausweisen ein Fälschungsrisiko bestehe. Im Vergleich dazu sei sie der Ansicht, dass die zusätzlichen Daten, die für die Aufnahme in das Register verlangt werden, das Verfahren in jedem Fall zuverlässiger machten als den Ausweis. SWT hob auch hervor, dass das Gesetz keine Formvorschriften für eine Willenserklärung zur Organspende kenne, dass

die Aufnahme in das Register auf freiwilliger Basis erfolge und dass das Register keine medizinischen Daten enthalte.

29 Weiter erklärte SWT, dass der Fall bei einem potenziellen Spendefall mit der Familie besprochen werde, der das Datenblatt vorgelegt wird. Laut SWT verringert dies das Fehlerrisiko weiter, da die Familie in der Lage sei, Unregelmässigkeiten (fragwürdige E-Mail-Adresse, Unterschrift usw.) zu erkennen.

30 SWT hatte vor der Einführung des Registers ein Rechtsgutachten einer Anwaltskanzlei zum Thema Datenschutz eingeholt. Die Möglichkeit der Registrierung über Smartphone/Tablet war jedoch nicht bewertet worden, da sie erst später eingeführt wurde. Die Einführung dieser Art der Registrierung zielte darauf ab, den Prozess zu vereinfachen, indem die physische Handlung – das Scannen oder Versenden des Datenblatts per Post – wegfiel, da dies zu vielen Verfahrensabbrüchen führte.

31 Schliesslich hat SWT angegeben, dass keine Überprüfung der bestehenden Profile auf ihre Authentizität geplant sei.

2.3. Registrierungsprozesse

2.3.1. Vorbemerkungen und Allgemeines

32 Vor der Einstellung der Registrierungsprozesse im Januar dieses Jahres gab es verschiedene Möglichkeiten, sich im NOSR zu registrieren: über einen Computer, ein Smartphone oder ein Tablet, wobei jede dieser Methoden auch Untervarianten hatte (vgl. Ziff. 2.3.2 und 2.3.3). SWT hat angekündigt, dass sie diese Verfahren abschaffen und durch ein einziges Verfahren ersetzen wird, das die von einem privaten Unternehmen angebotene Anwendung «[redacted]» verwendet (vgl. Ziff. 2.3.4). Dieser neue Prozess befindet sich noch in der Implementierungsphase.

33 Keine der bisherigen oder geplanten Registrierungsmethoden beinhaltet eine amtliche Überprüfung der Identität.

34 Sowohl bei den früheren Eintragungsmethoden wie auch beim geplanten Prozess mittels [redacted] kann pro E-Mail-Adresse nur ein einziges Profil erstellt verwendet werden. Es gibt zudem bei einer Eintragung keine Kontrolle diesbezüglich, ob eine Person bereits im Register verzeichnet ist; eine Person kann also durch die Verwendung mehrerer E-Mail-Adressen mehrere Profile anlegen. Allerdings wird auch das Datum der Registrierung bzw. der Aktivierung des Profils gespeichert. Falls für eine Person mehrere Profile vorliegen, kann so die aktuellste Willensbekundung ermittelt werden.

35 Sowohl bei den früheren wie auch bei der geplanten Eintragungsmethode werden Profile, bei denen der Registrierungsprozess nicht erfolgreich abgeschlossen werden konnte, nach drei Erinnerungen gelöscht.

2.3.2. Eintragung via PC und auf dem Postweg

36 Die Registrierung von einem Computer aus erfolgte über eine Online-Anwendung auf der Website von SWT (www.swisstransplant.org/register oder www.organspenderegister.ch). Die Erstellung eines Profils war in sechs Schritte unterteilt:

1. Eingabe der Basisdaten (Name, Vorname, Geburtsdatum, Heimatort, Adresse, Geschlecht, E-Mail-Adresse und Login-Daten);
2. Entscheid über die Organ-/Gewebespende oder Benennung einer Vertrauensperson;
3. Entscheid über die Spende für Forschungszwecke;
4. Eventuelle Nachricht an Angehörige;
5. Zusammenfassung;
6. Erstellung des Datenblatts, das die persönlichen Daten und den Entscheid über die Spende enthält.

37 Die Person bestätigte im letzten Schritt ihre Identität. Sie konnte zwischen zwei Methoden wählen:

- Die Person lud ein Foto von sich und einen Scan ihres Ausweises (amtlicher Ausweis wie Identitätskarte oder Pass) hoch und druckte das Datenblatt aus, das sie unterschreiben musste. Sie konnte es dann entweder fotografieren/scannen und in ihr Profil hochladen (Variante 1a) oder es per Post an SWT schicken (Variante 1b), wo es gescannt und in das Profil hochgeladen wurde.

- Postvariante (Variante 2): Das Datenblatt wurde von SWT ausgedruckt, die es der Person an die von ihr angegebene Adresse schickte. Die Person unterschrieb das Blatt und schickte es dann per Post an SWT zurück. SWT scannte das Blatt ein und lud es in das Profil der Person hoch. Bei dieser Variante dienten die Postadresse und die handschriftliche Unterschrift als Identifikationsmassnahmen – eine Ausweiskopie wurde in diesem Verfahren nicht verlangt.

38 SWT führte anschliessend je nach Variante die folgenden manuellen Überprüfungen durch:

- Bei den Varianten 1a und b prüfte SWT, ob die hochgeladenen Dokumente vollständig und lesbar waren, ob das Datenblatt unterschrieben war und ob die eingetragenen Daten (Name, Geburtsdatum, etc.) in den verschiedenen Dokumenten (Ausweis, Profil, Datenblatt) übereinstimmten. Der gescannte Ausweis wurde auf formale Gültigkeit geprüft; sollte der Scan des Ausweises fehlen oder dieser ungültig sein, erhielt die Person eine E-Mail, in der sie aufgefordert wird, eine Kopie eines gültigen Ausweises hochzuladen. Wenn die Unterschrift fehlte, wurde das Datenblatt per Post an die Person zur Unterschrift gesendet. Wenn die persönlichen Daten (Name, Geburtsdatum etc.) nicht übereinstimmten, wurde die Person per E-Mail darüber informiert und angewiesen, den Vorgang zu wiederholen.

- In der Variante 2 überprüfte SWT, ob das Datenblatt vollständig, lesbar und unterschrieben war, nachdem es zurückgeschickt wurde.

39 Es wird präzisiert, dass in den Varianten 1b und 2, d. h. wenn das Datenblatt per Post an SWT gesendet wurde, die Überprüfungen bezüglich des Datenblatts direkt auf dem Papier vorgenommen wurden. Das Blatt wurde dann gescannt und mithilfe eines Barcodes auf dem Blatt automatisch dem entsprechenden Profil zugeordnet. SWT führte Stichproben durch, um sicherzustellen, dass die Zuordnungen korrekt waren. Bei einem technischen Fehler (z.B. Barcode kann nicht gelesen werden) wurde das Datenblatt manuell dem richtigen Profil zugewiesen.

40 Wenn alles in Ordnung war, aktivierte SWT das Profil und machte es somit im Rahmen einer Anfrage im NOSR verfügbar. Die Person wurde darüber per E-Mail informiert.

2.3.3. Eintragung via Smartphone oder Tablet

41 Der im Folgenden beschriebene Prozess betraf die Registrierung über private Smartphones und Tablets, aber auch über die sog. CUBE, d.h. Registrierungsstellen mit Tablets, die an verschiedenen öffentlichen Orten (Kontaktstellen, hauptsächlich Spitäler und Kliniken) angeboten werden.

42 In Bezug auf die CUBE stellte SWT klar, dass das Personal der Kontaktstellen in keiner Weise in den Registrierungsprozess eingebunden war: Es stellte lediglich den technischen Betrieb des CUBE sicher und nahm eventuelle Rückmeldungen entgegen.

43 Der Prozess begann gleich wie bei der Registrierung über einen Computer, nämlich mit dem Start einer Anwendung, die unter den in der vorherigen Ziffer angegebenen Adressen erhältlich ist. Anschliessend lief der Prozess bis zum vierten Prozessschritt ab wie oben unter Ziff. 2.3.2 beschrieben:

1. Eingabe der Basisdaten (Name, Vorname, Geburtsdatum, Heimatort, Adresse, Geschlecht, E-Mail-Adresse und Login-Daten);
2. Entscheid über die Organ-/Gewebespende oder Benennung einer Vertrauensperson;
3. Entscheid über die Spende für Forschungszwecke;
4. Eventuelle Nachricht an Angehörige;

Anschliessend folgten die nächsten Prozessschritte:

5. Die Person machte ein Selfie mit dem Smartphone/Tablet;
6. Das anschliessend erstellte Datenblatt wurde direkt auf dem Bildschirm unterschrieben.

44 Die Person erhielt anschliessend eine automatische E-Mail, die ihren Benutzernamen und einen Link enthielt, mit dem sie ein Passwort erstellen musste. Nach der Erstellung des Passworts wurde ein Bestätigungs-E-Mail verschickt.

45 SWT überprüfte in der Anwendung, ob die Qualität des Selfies und der Unterschrift ausreichend war. Wenn alles in Ordnung war, aktivierte SWT das Profil und machte es somit im Rahmen einer Anfrage im NOSR verfügbar. Die Person wurde darüber per E-Mail informiert.

46 Sollte das Selfie oder die Unterschrift fehlen oder von schlechter Qualität sein, wurde der Registrierungsprozess auf dem Postweg abgeschlossen, d. h. wie in Variante 2 oben: SWT schickte das Datenblatt per Post an die angegebene Adresse, die Person unterschrieb es und schickte es per Post zurück. Parallel dazu wurde die Person per E-Mail darüber informiert.

47 Diese Eintragungsvariante via Smartphone bzw. Tablet war im Bericht ZFT beschrieben und im Rahmen der journalistischen Recherche verwendet worden, um ein Profil im Namen des SRF-Journalisten zu erstellen. Das Selfie wurde Mithilfe eines frei im Internet zugänglichen Fotos fingiert. Die verwendete E-Mail-Adresse war insofern eine Fälschung, als sie eigens für die Zwecke der Recherche erstellt worden war.

2.3.4. Neuer Registrierungsprozess mithilfe von «[redacted]»

48 SWT beabsichtigt, alle oben beschriebenen Registrierungsprozesse abzuschaffen und durch eine einzige Lösung zu ersetzen, bei der die vom privaten Unternehmen [redacted] AG angebotene Anwendung für die Authentifizierung des Nutzers (nachfolgend "[redacted]") verwendet wird.

49 Der Prozess wird von einem Smartphone/Tablet oder einem Computer aus gestartet werden können und wird sich gemäss den Ausführungen von SWT und [redacted] AG wie folgt präsentieren:

1. Die Person öffnet eine App von der Swisstranplant-Website. Sie gibt ihre Koordinaten ein (Name, Vorname, Geburtsdatum usw.).
2. Die App startet dann den Prozess zur Überprüfung der Identität der Person, einen sog. Liveness-Check: [redacted] fordert den Nutzer bzw. die Nutzerin dazu auf, vier Selfies aus verschiedenen Perspektiven (frontal, im Profil, frontal lächelnd) zu machen und anschliessend einen Ausweis zu fotografieren. [redacted] gleicht die manuell gemachten Angaben mit den Angaben des Ausweises ab und bestätigt bei Übereinstimmung die Identität der Nutzerin bzw. des Nutzers.
3. Die Person gibt dann ihre Entscheidung zu Organ- und Gewebespenden sowie über die Verwendung zu Forschungszwecken an.
4. Das Datenblatt wird erstellt und direkt auf dem Bildschirm oder, falls kein Touchscreen verfügbar ist, mit der Maus unterschrieben.
   Es besteht auch die Möglichkeit, das Datenblatt in diesem Zeitpunkt auszudrucken, zu unterschreiben, einzuscannen und in das Profil hochzuladen oder es per Post an SWT zu schicken, wo es dann, wie bei den alten Verfahren, von SWT hochgeladen würde.
5. Sobald der Vorgang abgeschlossen ist, wird eine Bestätigungs-E-Mail an den Interessenten gesendet. Bei dieser Gelegenheit muss er auch ein Passwort, sowie einen zweiten Identifikationsfaktor (im Prinzip die SMS, siehe Ziff. 2.4) festlegen, um später auf sein Profil zuzugreifen.

50 Anzumerken ist, dass der Liveness-Check über ein Smartphone durchgeführt wird, auch wenn der Prozess von einem Computer gestartet wird. Ein QR-Code, der auf dem Bildschirm des Computers generiert wird, stellt die Verknüpfung zwischen den beiden Medien her. Dieser Prozess soll auch für CUBEs verwendet werden, die Beibehaltung und ggf. die Gestaltung dieser CUBEs ist jedoch noch in der Diskussion.

51 Sobald die Registrierung abgeschlossen ist, prüft SWT, ob die Qualität des Fotos auf dem Datenblatt bzw. der Unterschrift ausreichend ist. Ist dies in Ordnung, prüft SWT, ob das Ergebnis der Identifizierung durch [redacted] zu 100% validiert ist. Ist dies nicht der Fall, nimmt SWT eine manuelle Überprüfung vor: Ein Ergebnis unter 100% kann etwa durch einen Tippfehler, die Eingabe nur eines Vornamens, obwohl die ID zwei Vornamen angibt, usw. erklärt werden. Wenn die Identität auf diese Weise zweifelsfrei bestätigt werden kann, wird das Profil im Register aktiviert.

52 Falls die Registrierung nicht validiert werden kann, wird die Person schriftlich oder telefonisch darüber informiert. Sie wird dann aufgefordert, den Fehler zu korrigieren oder das Verfahren zu wiederholen – das erste Profil wird parallel dazu gelöscht. Ein nicht bestätigtes Profil wird nach drei Monaten gelöscht, worüber die Person informiert wird. Anfragen mit einem zu niedrigen Liveness-Check-Score werden nicht an SWT weitergeleitet. Der Nutzer erhält dann eine Nachricht, dass der Prozess nicht erfolgreich abgeschlossen werden konnte.

53 Sobald das Profil validiert wurde, aktiviert SWT das Profil und macht es damit für Abfragen im NOSR verfügbar. Die Person wird darüber per E-Mail informiert.

54 SWT speichert die von [redacted] im Rahmen des Registrierungsprozesses erhobenen Daten. Die beim Liveness-Check aufgenommenen Fotos und je ein Foto der Vor- und Rückseite des Ausweisdokuments werden auf einem PDF-Dokument übermittelt und im Register abgespeichert. Daneben wird ein Foto des Ausweises in hoher Auflösung separat abgespeichert. Gemäss SWT diene dieses hochauflösende Ausweisfoto dazu, im Falle späterer Zweifel über die Identität des Nutzers darauf zurückgreifen zu können.

55 SWT erklärt, dass es nicht möglich sein wird, ein Profil zu erstellen, ohne den Authentifizierungsprozess von [redacted] durchlaufen zu haben, und zwar auch nicht für die eigenen Mitarbeiter.

56 Beim Authentifizierungsprozess handelt es sich um eine von der [redacted] AG entwickelte Anwendung. Sie soll eine zuverlässige Authentifizierung aus der Distanz ermöglichen. Laut [redacted] AG entspricht die Anwendung der FINMA-Richtlinie 2016/7[2], ein Punkt, der von der Firma KPMG auditiert wurde. Die Infrastruktur von Begasoft AG – zertifiziert nach ISO 27001 und 9001, siehe unten 2.8.2 – beherbergt die Aktivitäten von [redacted] AG. [redacted] AG löscht die Daten, die ihr im Rahmen der Authentifizierung übermittelt werden, nach 14 Tagen vollständig; dieser Zeitraum wurde so festgesetzt, dass er die Schliessungszeiten von SWT (etwa während der Festtage) berücksichtigt. Das Ergebnis der Authentifizierung durch [redacted] wird zwar automatisch an SWT gesendet, aber bei Problemen muss SWT möglicherweise [redacted] AG kontaktieren.

57 Gemäss SWT ist noch offen, ob bzw. ab wann der Identifikationsprozess mittels [redacted] implementiert wird.

[2] Rundschreiben 2016/7 «Video- und Online-Identifizierung» vom 3. März 2016, abrufbar unter https://finma.ch/de/dokumentation/rundschreiben/

2.4. Zugang zum eigenen Registereintrag

58 Sobald eine Person im NOSR registriert ist, kann sie über ein Zwei-Faktor-Identifikationsverfahren (2FA) auf ihr Profil – und damit auf ihre Daten im Register – zugreifen. Der erste Faktor ist ein Passwort, das im Zuge des Registrierungsverfahrens festgelegt wird. Der zweite Faktor ist ein Code, den der Nutzer per E-Mail oder SMS erhält, je nachdem, was er ausgewählt hat.

59 Bei Verlust des Passworts kann durch ein Wiederherstellungsverfahren unter Verwendung der E-Mail-Adresse ein neues Passwort erhalten werden. In ihrem Schreiben vom 8. Februar 2022, das der Stellungnahme von SWT vom 18. Februar 2022 beigefügt war,hält Begasoft AG die 2FA-Identifikation für sicher. Sie erwägt jedoch, auf die E-Mail-Adresse zu verzichten und künftig nur noch SMS als zweiten Faktor zu verwenden.

60 Der Zugang zum Konto ermöglicht es den Nutzern, ihre Daten (Adresse usw.) und ihren Entscheid zum Spendewillen zu ändern. In diesem letzten Fall müssen sie ein neues Datenblatt ausfüllen und unterschreiben, das dann in ihr Profil hochgeladen wird. Es gibt allerdings kein neues Authentifizierungsverfahren mit Selfie oder ID (bzw. künftig [redacted]), es ist nur der Zugang zum Konto über die 2FA-Identifikation erforderlich.

2.5. Ablauf im Fall einer potentiellen Organentnahme

61 Damit eine Organentnahme in Betracht gezogen werden kann, müssen nach geltendem Recht zwei Bedingungen erfüllt sein: Der Patient muss sich in einer infausten Prognose oder einem beschlossenen Therapieabbruch befinden und er muss der Organentnahme zugestimmt haben. In diesem Kontext, in dem versucht wird, den Willen des Patienten – unter Miteinbezug seiner Angehörigen – zu ermitteln, kommt ein allfälliger Eintrag im NOSR zum Einsatz. Der Ablauf ist dann wie folgt:

1. Das betroffene Spital setzt sich telefonisch mit dem SWT-Koordinierungszentrum in Verbindung.
2. Der SWT-Operator (im Folgenden NC für National Coordination) prüft, ob die anrufende Person berechtigt ist, die gewünschte Information zu erhalten. Zu diesem Zweck wird sie nach ihrem Namen, Vornamen, ihrer Funktion und dem Krankenhaus, für das sie arbeitet, sowie nach der direkten Telefonnummer und einer E-Mail-Adresse gefragt (es muss sich um eine offizielle Telefonnummer und eine offizielle E-Mail-Adresse des Spitals handeln). Nur akkreditierte Ärzte oder Pflegefachpersonen, sowie das Koordinationspersonal einer anerkannten IPS (oder Notfallstation) eines Schweizer Spitals sind auskunftsberechtigt. Abfragen aus dem Ausland haben über national zuständige Organisation zu erfolgen (z. B. ABM).

3. Sofern die anfragende Person der NC nicht persönlich bekannt ist, ruft die NC sofort die Zentrale des betreffenden Krankenhauses zurück und bittet um Verbindung mit der anfragenden Person. Dadurch soll die Identität des Anfragenden sichergestellt werden.
4. Nachdem die Identität des Anrufers bestätigt wurde, wird er aufgefordert, den Status des Patienten zu bestätigen, d.h., dass er eine infauste Prognose hat. Der Antragsteller wird auch darüber informiert, dass jede Anfrage an das NOSR registriert wird und dass der potenzielle Spender innerhalb von 48 Stunden eine Informations-E-Mail erhält, um einen möglichen Missbrauch aufzudecken.
5. Der NC sucht den Patienten im Register. Dazu muss der Antragsteller ihm den Namen, Vornamen und das Geburtsdatum mitteilen; die Daten müssen genau mit denen im Register übereinstimmen.
6. Wenn der Patient im Register eingetragen ist, wird das Datenblatt in einem verschlüsselten PDF-Format generiert, zusammen mit dem Code, mit dem es entschlüsselt werden kann. Dieser Code wird der antragstellenden Person telefonisch mitgeteilt. Gleichzeitig wird das Datenblatt per E-Mail über Outlook an die Adresse des Antragstellers gesendet. Gegebenenfalls wird das Datenblatt vom medizinischen Personal mit den Angehörigen besprochen. Schliesslich werden die unter Ziff. 2 aufgeführten Daten des Antragstellers in der NOSR-Applikation gespeichert.

62 Parallel zu diesem Prozess werden die Anfragen an das Register auch in einer Power App "Abfrage NOSR" von Microsoft gespeichert. Dabei handelt es sich um eine vom Register unabhängige Applikation, deren Zugriff über eine Zwei-Faktoren-Authentifizierung erfolgt. Sie soll Qualitätskontrollen der Organspendeprozesse ermöglichen. Folgende Daten werden dort eingegeben: Name, Vorname, Geburtsdatum und der Entscheid des Patienten. Wird der Patient zur Spenderin oder zum Spender, wird der Eintrag mit der SOAS-ID (Swiss Organ Allocation System) ergänzt. Anfragen, die sich auf eine Person beziehen, die nicht im NOSR registriert ist, werden auch in der Power App erfasst.

63 Der Prozess beschreibt die Rolle des NOSR und folglich von SWT in Bezug auf die Ermittlung des Patientenwillens. Es sei daran erinnert, dass SWT auch die Verteilung der verfügbaren Organe verwaltet, so dass die Ermittlung des Patientenwillens nur ein Teil der Aktivitäten von SWT und des Transplantationsprozesses ist.

2.6. Löschung von Einträgen im Register

64 Die Löschung von Einträgen im NOSR erfolgt in drei Fällen:

- wenn die Person ihr Profil selber löscht, was jederzeit mittels Login in das eigene Konto möglich ist;
- wenn eine registrierte Person das Alter von 95 Jahren erreicht, löscht SWT das Profil; in diesem Fall wird eine Informations-E-Mail an die angegebene Adresse gesendet;
- falls SWT, beispielsweise durch die Meldung von Angehörigen, Kenntnis vom Tod einer eingetragenen Person erhält; in diesem Fall wird ein Todesschein angefordert.

65 In diesen Fällen werden die Daten vollständig und physisch auf den Servern gelöscht. Sie werden jedoch in den Backups aufbewahrt, da SWT nicht in der Lage ist, gezielte Löschungen in den Archiven vorzunehmen. Die Daten in den Backups werden verschlüsselt und netzwerkunabhängig gespeichert. Backups werden vier Wochen lang aufbewahrt und dann gelöscht.

66 Die NOSR wird nicht mit anderen Datenbanken von anderen Stellen (z. B. dem Einwohnermeldeamt) koordiniert. Daher erfährt SWT ausserhalb von potenziellen Spendenverfahren nicht notwendigerweise vom Tod einer registrierten Person.

67 Papierdokumente (insbesondere physische Datenblätter), die im Rahmen der Anmeldung anfallen, werden gemäss Ausführungen von SWT fachgerecht entsorgt.

2.7. Datenbearbeitung und -zugriff durch SWT

68 SWT bearbeitet die Daten von Personen, die im Register eingetragen sind, nur bei zwei Gelegenheiten aktiv: bei der Registrierung und bei einer Anfrage an das Register. In ihren AGB, die während des Registrierungsprozesses akzeptiert werden müssen, behält sich SWT das Recht vor, die Daten für analytische und statistische Zwecke in anonymisierter Form zu verwenden. In diesem Umfang behält sie sich auch das Recht vor, die Daten an Dritte weiterzugeben.

69 Im Übrigen greift SWT nicht auf die Daten zu und nimmt nach erfolgreicher Eintragung (ausser für grundlegende Informationen, die alle Eingetragenen betreffen) keinen Kontakt mit den Eingetragenen auf. Eventuelle Änderungen (Änderung des Wohnsitzes, des Willens usw.) werden direkt von den angemeldeten Personen vorgenommen.

2.8. Datensicherheit und IT

2.8.1. Sicherheitslücken gemäss Bericht ZFT

70 Laut dem Bericht ZFT war es aufgrund einer fehlenden Validierung möglich, auf die Daten des Servers zuzugreifen, der das Register beherbergt. SWT bzw. Begasoft AG räumten die Existenz der Lücke ein, schlossen aber aus, dass dadurch der Zugriff auf persönliche Daten möglich gewesen sei, denn um die Lücke auszunutzen, hätte man den Pfad und Dateinamen genau kennen müssen. Diese Elemente seien bei personenbezogenen Daten jedoch nicht zu erraten. Somit konnten nur Systemdaten abgefragt werden, für die Standard-Pfad- und Dateinamen verwendet werden.

71 Das Eindringen in das System durch ZFT war von der Firewall zwar erkannt, aber nicht blockiert worden. Die Lücke wurde inzwischen durch die Einführung eines zusätzlichen Validierungsprozesses und eine neue Einstellung der Firewall behoben. Laut Begasoft AG steht fest, dass es ausser dem Zugriff von ZFT in den letzten zwei Monaten (ausgehen vom Datum ihrer Stellungnahme vom 8. Februar 2022) keine weiteren unberechtigten Zugriffe gegeben hat.

2.8.2. Allgemeine Ausführungen zur IT-Infrastruktur

72 Bisher wurden keine externen Sicherheitsprüfungen der Datenbank oder der Webapplikation des NOSR durchgeführt. SWT kündigt an, dass nach der Einführung der neuen Authentifizierungslösung ([redacted]) solche Audits regelmässig durchgeführt werden sollen.

73 Die Begasoft AG ist nach ISO 9001 und ISO 27001 zertifiziert.

74 Es wird ein Logbuch geführt, sowohl für die Angestellten von SWT als auch für die Benutzer. Jede Operation am Register wird dort dokumentiert, einschliesslich erfolglose Anmeldeversuche. Bei Verdacht auf Unregelmässigkeiten oder in besonderen Fällen werden die Logs überprüft.

75 Im Übrigen hat der EDÖB keine Detailuntersuchung der IT-Prozesse durchgeführt und konnte insbesondere kein definitives Schema zum neu geplanten Registrationsprozess einsehen, da sich der [redacted]-Prozess noch in der Implementierungsphase befindet. Auf der Grundlage der erhaltenen Informationen scheinen das IT-System und die Verwaltung der Backups jedoch angemessen und kohärent aufgebaut zu sein. Sie weisen keine offensichtlichen Lücken auf.

3. Rechtliche Würdigung und Empfehlungen

3.1. Datensicherheit und insb. Datenrichtigkeit

76 Gemäss Art. 7 DSG i.V.m. Art. 8ff. VDSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Wer Daten bearbeitet, hat für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten zu sorgen. Zudem muss er sicherstellen, dass die verarbeiteten Daten inhaltlich richtig sind (Art. 5 Abs. 1 DSG).

77 Im vorliegenden Fall war der letztgenannte Aspekt besonders problematisch. Der Bericht ZFT zeigte auf, dass es relativ einfach war, im Namen einer anderen Person und ohne deren Wissen ein Profil zu erstellen und eine Erklärung zur Organspende abzugeben. Mit anderen Worten war die Richtigkeit der Daten nicht gewährleistet, da die aufgezeichnete Willenserklärung möglicherweise nicht von der betroffenen Person stammte und damit auch nicht unbedingt dem tatsächlichen Willen der betroffenen Person entsprach.

78 Bei einer Willenserklärung zur Organspende handelt es sich um eine Entscheidung, die von sehr persönlichen Ansichten abhängt; es geht um Leben, um Tod und um die Integrität des Körpers, also um Aspekte, die von den einzelnen Personen sehr unterschiedlich betrachtet werden. Die Willenserklärungen sind als Daten über die Intimsphäre und damit um besonders schützenswerte Daten im Sinne von Art. 3 Bst. c Ziff. 2 DSG zu betrachten. Dementsprechend ist die Richtigkeit und Authentizität der im Register abgegebenen Erklärung umso wichtiger.

79 Die Tatsache, dass das Gesetz keine bestimmte Form vorsieht, um seinen Willen festzuhalten, ist vorliegend nicht relevant. Das Problem ist nämlich nicht die rechtliche Gültigkeit einer solchen Erklärung, sondern ihre Verlässlichkeit. Indem SWT der Öffentlichkeit ein spezielles Register zur Verfügung stellt, übernimmt sie die Verantwortung für dieses Instrument. Dies gilt umso mehr im Hinblick auf die Rolle des Registers als zentrale Datenbank, auf die im Falle einer potenziellen Spende durch die Spitäler systematisch zurückgegriffen wird. Dieses Register ist umso bedeutender, als es von der nationalen Zuteilungsstelle geführt wird, die, wie bereits erwähnt, ein wesentlicher Akteur in jedem Transplantationsverfahren ist.

80 SWT war sich bewusst, dass das bisherige System nicht vollkommen sicher war (vgl. oben Ziff. 2.2). Sie habe jedoch das Ziel verfolgt, das Registrierungssystem relativ einfach zu gestalten, um möglichst viele Menschen zu erreichen. SWT betonte auch, dass ein Täter keinen Nutzen aus einer solchen Fälschung ziehen könne – es würde einer bestimmten Person nicht ermöglichen, ein Organ zu erhalten. Sie beurteilte das Risiko daher nicht als wesentlich.

81 Diesem Ansatz kann aus datenschutzrechtlicher Perspektive nicht zugestimmt werden. Zunächst muss unabhängig von den Fragen des Motivs festgestellt werden, dass vorliegend um besonders schützenswerte Personendaten geht und die technische Möglichkeit, Profile unter dem Namen eines Dritten zu erstellen, ohne besondere Hardware oder Computerkenntnisse realisierbar war. Aus datenschutzrechtlicher Sicht reicht dies allein schon aus, um das System als unzureichend zu bezeichnen. Die Zuverlässigkeit des Systems war technisch nicht gewährleistet. Was die Motivation des Täters betrifft, so kann man nicht davon ausgehen, dass niemand diese Schwachstelle ausnutzen wird, weil er scheinbar keinen direkten Nutzen daraus ziehen kann. Neben dem rein schikanösen oder schädlichen Aspekt sind z.B. auch militante oder systemfeindliche Gründe denkbar. Die Motive einer Person können vielfältig sein und man kann sie nicht einfach aberkennen, nur weil sie nicht vernünftig erscheinen. Auch soll die Zuverlässigkeit eines Systems nicht einfach auf dem Wohlwollen der Bevölkerung beruhen können. Dies gilt umso mehr, als offensichtlich ist, dass die festgestellten Mängel geeignet waren, das Vertrauen der Öffentlichkeit in das System der Organspende in der Schweiz in der demokratiepolitisch sensiblen Zeitspanne vor der eidgenössischen Abstimmung vom 15. Mai 2022 zu beeinträchtigen.

3.2. Authentifizierungsprozess

82 Die Frage nach der Authentizität von Profilen bezieht sich auf die Mechanismen der Registrierung, d.h. auf ihre Zuverlässigkeit in Bezug auf die Kontrolle der Identität des Nutzers.

83 Wie oben ausgeführt (vgl. Ziff. 2.3), konnte man sich auf drei verschiedene Arten in das Register eintragen: per Computer, auf dem Postweg oder per Tablet und Smartphone (die Variante, die ZFT zur Erstellung eines fingierten Profils nutzte). Nur bei der ersten dieser Varianten wurde eine Ausweiskopie verlangt. Bei der zweiten Variante wurde die Zustellbarkeit an die angegebene Adresse als Identitätsprüfung angesehen. Bei der dritten Variante hatte das Selfie diese Funktion. Ausserdem wurde eine Unterschrift verlangt, je nach Variante handschriftlich oder digital.

84 Diese drei Verfahren wurden von SWT bereits eingestellt. Sie werden deshalb nicht im Detail kommentiert. Der EDÖB hält jedoch fest, dass keine dieser Lösungen eine echte Identitätskontrolle zum Zeitpunkt der Anmeldung beinhaltete. Die Vorlage einer gescannten ID belegt nicht, wer der Nutzer ist. Dies gilt auch für die Postadresse, da es möglich ist, eine falsche Adresse anzugeben und den Namen der betreffenden Person an den Briefkasten zu kleben (die Post führt keine vorgelagerte Adressprüfung durch). Was die Smartphone-/Tablet-Lösung betrifft, wird auf das Anwendungsbeispiel von ZFT bzw. der Sendung Kassensturz verwiesen. Zwar hält SWT dagegen, dass in einer

potenziellen Spendensituation die Angehörigen gewisse Unregelmässigkeiten erkennen können. Dies sei jedoch keine Garantie, zumal die Angehörigen nicht immer anwesend seien.

85 Der EDÖB ist daher der Ansicht, dass diese alten Verfahren keine ausreichende Sicherheit boten; ihre Aufhebung und die geplante gänzliche Abschaffung sind daher gerechtfertigt.

86 Um diese Mängel zu beheben, erwägt SWT, die Anwendung [redacted] einzusetzen. Diese basiert auf einem Liveness-Check-Verfahren, das mehrere Fotos und die Vorlage eines Ausweisdokuments (das Dokument selbst, eine Kopie reicht nicht aus) umfasst (vgl. oben Ziff. 2.3.4).

87 Der «Online Identification Service» der [redacted] AG wurde von KPMG im Jahr 2019 auditiert[3]. Bei dieser Prüfung wurde der Prozess insbesondere mit den Anforderungen des FINMA-Rundschreibens 2016/7 abgeglichen. Der Prüfbericht hält fest, dass der Prozess insgesamt mit dem Rundschreiben übereinstimmt, auch wenn er nicht alle Anforderungen erfüllt, u.a. in Bezug auf die in Ziff. 31.4 des Rundschreibens geforderte Archivierung der Identifikationsdokumente. Unter Datenschutzaspekt ist dieser Punkt und im vorliegenden Kontext eher positiv zu bewerten.

88 Hingegen sieht SWT vor, die Daten aus dem [redacted]-Prozess zu speichern, d.h. die Fotos des Gesichts und des Ausweises im PDF, welches das Durchlaufen des [redacted]-Prozesses dokumentiert und daneben ein Ausweisfoto in hoher Auflösung. SWT gehe es dabei darum, die Gültigkeit eines Eintrags beweisen zu können, falls sich nach einem Todesfall diese Frage stellen sollte. In Kontext des NOSR ist die Aufbewahrung eines hochauflösenden Bilds des Ausweises allein zu diesem Zweck jedoch zu weitgehend und mit zusätzliche Risiken verbunden, ohne dass ein Mehrwert ersichtlich wäre.

89 Im Sinne der Datensparsamkeit wäre zudem anstelle des PDF-Dokuments mit den Portraitaufnahmen und dem Ausweisfoto gegebenenfalls eine elektronische Bescheinigung bzw. Signatur im Betracht zu ziehen, die belegt, dass der [redacted]-Identifizierungsprozess tatsächlich durchlaufen wurde.

[3] KPMG, Independent Reasonable Assurance Report to [redacted] GmbH on the Company's "Online Identification Service" der KPMG vom 28. Juni 2019

Empfehlungen betreffend Identifikationsprozesse:

1a. Die früher angebotenen Identifikationsprozesse sind nicht wieder aufzunehmen.

1b. Der neue Identifikationsprozess mit Einbezug von [redacted] ist wie angekündigt umsetzen, unter Vorbehalt von Bst. c sogleich.

1c. Es ist auf die Speicherung eines hochauflösenden Bilds des Ausweises im Register zu verzichten.

1d. Die Möglichkeit der Neuregistierungen ist erst wieder aufzuschalten, wenn die Anpassungen in Bezug auf die Registrierungsprozesse umgesetzt worden sind.

3.3. Bearbeitung und Pflege bestehender Registereinträge

90 Jede im NOSR registrierte Person kann sich über einen Zwei-Faktoren-Authentifikationsprozess in ihr Profil einloggen, wo Änderungen der Kontaktdaten direkt vorgenommen werden können. Dies gilt sowohl für Personen, die sich nach den früheren Eintragungsprozessen registriert hatten, und soll auch künftig wieder möglich sein. Bei einer Änderung des Spendenwillens ist ein neues Datenblatt erforderlich. Neben dem Passwort war der zweite Faktor ein Code, der per E-Mail oder SMS mitgeteilt wurde. Obwohl Begasoft AG in ihrem Schreiben vom 8. Februar 2022, das der Stellungnahme von SWT vom 18. Februar 2022 beigefügt war, beide Methoden als sicher bezeichnete, schlug sie dennoch vor, auf die Authentifizierung per E-Mail zu verzichten.

91 Der EDÖB teilt die Ansicht, dass die Verwendung der E-Mail als zweiter Faktor ein geringeres Sicherheitsniveau aufwies als die SMS. Denn wenn das Passwort vergessen wird, läuft der Wiederherstellungsprozess über die E-Mail. Wenn also jemand die E-Mail-Adresse des Nutzers gehackt hat, kann er das Passwort ändern und dann auf das Profil zugreifen: die beiden Faktoren sind also nicht unabhängig voneinander. Der EDÖB ist daher der Ansicht, dass diese Änderung erforderlich war.

92 SWT hat angegeben, dass pro E-Mail-Adresse nur ein Profil erstellt werden kann. Dagegen gibt es keine Kontrolle über die Identität der Person in dem Sinne, dass sich eine Person mehrfach registrieren kann. Dadurch wird die Aussagekraft und damit Qualität der Daten geschmälert, weil unter Umständen von einer Person mehrere, theoretisch auch widersprüchliche Einträge bestehen können.

93 Um Mehrfachanmeldungen zu vermeiden und damit insbesondere dem Anspruch der Datenrichtigkeit gerecht zu werden, wäre deshalb eine Kontrolle wünschenswert. Sollte das nicht umsetzbar

sein, sollte bei einer Anfrage an das Register ein Verfahren eingeführt werden, das sicherstellt, dass alle Einträge berücksichtigt werden, sofern es mehrere Profile für dieselbe Person gibt. Dabei sollte erkennbar sein, welches das neueste ist und somit die aktuellste Aussage enthält.

94 Im Allgemeinen erklärte SWT, dass sie die registrierten Personen nach erfolgreicher Eintragung in der Regel nicht erneut kontaktiert. Allerdings kann ein Registereintrag unter Umständen erst Jahrzehnte später Wirkung entfalten. Dies kann dazu führen, dass eine Person ihre Meinung über die Organspende ändert, ohne sich daran zu erinnern, dass sie eine Erklärung im Register abgegeben hatte. Das Register würde dann eine inhaltlich falsche Information enthalten, was den Aspekt der Datenrichtigkeit im Sinne von Art. 5 DSG beschlägt.

95 Der Inhaber der Datensammlung, vorliegend SWT, trägt die Verantwortung für die Richtigkeit der von ihm bearbeiteten Daten; wie oben ausgeführt hat SWT jedoch nur eine beschränkte Möglichkeit, auf die Aktualität und Qualität der einzelnen Datensätze einzuwirken. Als Verantwortliche hat sie jedoch Massnahmen zu ergreifen, um die Datenqualität bestmöglich zu gewährleisten, konkret indem die Nutzerinnen und Nutzer zur Datenpflege angehalten bzw. in regelmässigen Abständen kontaktiert und daran erinnert werden.

96 Auch angesichts der erstellten Mängel in Bezug auf die Identifikation und die daraus entstandene Möglichkeit, Einträge in fremdem Namen zu erstellen, hat SWT mögliche Massnahmen zu prüfen und zu ergreifen. Dies wird insbesondere relevant werden, wenn eine allfällige Überführung der Daten in ein künftiges, vom Bund zur Verfügung gestelltes Register zur Diskussion stehen sollte. Da hierzu im Zeitpunkt der Redaktion des vorliegenden Berichts aber noch keine hinreichend konkretisierten Angaben bestehen, sieht der EDÖB vorläufig von entsprechenden Empfehlungen ab.

Empfehlungen betreffend Pflege der Einträge:

2a. Die geplante Anpassung des Zwei-Faktoren-Authentifizierungsprozesses ist so umzusetzen, dass die beiden Faktoren tatsächlich unabhängig voneinander sind (insb. Verzicht auf E-Mail als zweiten Faktor).

2b. Die im Register eingetragenen Nutzerinnen und Nutzer sind regelmässig zu kontaktieren und zur Pflege des eigenen Eintrags aufzufordern.

2c. Es sind Massnahmen zu treffen, um sicherzustellen, dass sich eine Person nur einmal registrieren kann bzw. dass bei einer Anfrage an das Register jeweils auf das aktuellste Profil Bezug genommen wird.

3.4. Änderung des Spendewillens

97 Das Gegenstück zur behandelten Sicherheit des Registrierungsprozesses ist die Sicherheit des Profils, wenn es einmal erstellt wurde. Diese Sicherheit betrifft sowohl unberechtigte Manipulationen durch Dritte als auch durch Mitarbeitende von SWT. Der Zugriff der Nutzerinnen und Nutzer auf das Profil wird durch eine Zwei-Faktor-Identifikation geschützt. Darüber hinaus wird jede Operation am Register durch die Nutzerin oder den Nutzer oder das Personal von SWT protokolliert. Der 2FA-Prozess ist jedoch nicht so zuverlässig wie der [redacted]-Prozess und verhindert nicht mögliche Back-Office-Aktionen der Mitarbeitenden von SWT, die ihre eigenen Zugänge haben. Was das Logbuch betrifft, so wird es in einer potenziellen Spendensituation nicht konsultiert und gibt nicht unbedingt Aufschluss über die Legitimität einer früher erfolgten Änderung.

98 Um seinen Spendewillen zu ändern, war es bislang nicht notwendig und wird es auch künftig nicht notwendig sei, erneut einen Authentifizierungsprozess zu durchlaufen. Es reicht, sich in sein Profil einzuloggen, die Änderung vorzunehmen und das neue Datenblatt zu unterschreiben. Der Spendewille kann als relevanteste Information im Register bezeichnet werden, insbesondere im potentiellen Spendenfall. Folglich muss sie besonders geschützt werden. Es ist etwa auch nicht ersichtlich, weshalb Mitarbeiter von SWT diese Information ändern können müssen. In der aktuellen Situation ist das Sicherheitsniveau für die Änderung dieses Willens jedoch niedriger als für seine ursprüngliche Eingabe, was das gesamte System schwächt. Der Schutz dieser Information vor unberechtigten Änderungen muss daher verstärkt werden. Eine Lösung, die einfach erscheint und zudem sowohl gegenüber Dritten als auch gegenüber Mitarbeitenden von SWT wirksam wäre, wäre die Verwendung des [redacted]-Prozesses auch für eine Änderung des Willens. Der zusätzliche Aufwand scheint vertretbar, zumal eine Willensänderung nicht leichtfertig und regelmässig vorgenommen wird.

99 Die hier gemachten Aussagen gelten auch für das Löschen von Profilen durch die betroffene Person selber – ein Vorgang, der die gleichen Auswirkungen haben kann wie eine Willensänderung.

Empfehlung betreffend Identifikation bei der Änderung des Spendewillens:

3 Bei jeder den Spendewillen betreffenden Bearbeitung durch die Nutzerinnen und Nutzer (Ersteintragung wie auch spätere Änderung) ist ein gleichwertiges Sicherheitsniveau in Bezug auf die Identifizierung zu gewährleisten.

4. Stellungnahme von Swisstransplant und Beurteilung durch den EDÖB

100 Mit Schreiben vom 15. Juli und 31. August 2022 nahm SWT im Rahmen der Gewährung des rechtlichen Gehörs Stellung zum vorliegenden Bericht (Stand am 17. Juni 2022) und insbesondere zu den Empfehlungen unter Ziffer 3 hiervor. In diesem Zusammenhang gab SWT bekannt, dass die Registereintragungen nicht wieder ermöglicht werden und dass die Umsetzung des Prozesses mit [redacted] somit nicht erfolgen werde. Sie wies jedoch darauf hin, dass das Register für Spitäler weiterhin zur Einsichtnahme zur Verfügung stehen werde. Darüber hinaus erklärte SWT, dass es nicht mehr möglich sein werde, seinen Willen in bestehenden Profilen zu ändern, sondern nur noch, diese zu löschen, was von SWT empfohlen werde, wenn die Person ihren im Profil hinterlegten Willen ändern möchte.

101 Der Entscheid der Stiftung, die Möglichkeit der Neuregistrierung nicht wieder zu öffnen, wirkt sich auf einige der Empfehlungen im vorliegenden Bericht aus. Während ein Teil der Empfehlungen weiterhin anwendbar bleibt (1a, 1d, 2a und 2c), ändert sich der Umfang anderer Empfehlungen (2b und 3), andere werden wiederum gegenstandslos (1b und 1c). Die Stellungnahme von SWT sowie gegebenenfalls die Anmerkungen des EDÖB dazu werden im Folgenden erläutert.

102 Die Empfehlungen 1a und 1d werden von SWT angenommen. Die Empfehlungen 1b und 1c, die sich speziell auf die Umsetzung des Prozesses mit [redacted] beziehen, sind durch den Entscheid, den entsprechenden Identifikationsprozess nicht wie geplant einzuführen, gegenstandslos geworden.

103 Empfehlung 2a wird von SWT abgelehnt, wofür SWT praktische Gründe anführt: Für etwa 55’000 Registereinträge lägen gar keine oder keine Schweizer Mobiltelefonnummern vor, so dass eine Umsetzung sehr schwierig erscheine. Darüber hinaus wies SWT die in ihrer Stellungnahme vom 18. Februar 2022 enthaltene Aussage ihres IT-Dienstleisters zurück, wonach die Identifizierung per E-Mail eingestellt werden solle. Infolgedessen bleibt diese Sicherheitslücke bestehen.

104 Die Empfehlung 2b bleibt aufgrund des Entscheids von SWT nur teilweise umsetzbar. SWT beabsichtigt, die registrierten Personen spätestens dann wieder zu kontaktieren, wenn das neue Register des Bundes eingerichtet werde. Die Empfehlung wurde daher angenommen, soweit sie noch umsetzbar ist.

105 Die Empfehlung 2c wird von SWT bereits umgesetzt, so dass sie als angenommen gelten kann.

106 Empfehlung 3 ist schliesslich nur noch teilweise umsetzbar, da die Änderung von Profilen nicht mehr möglich ist und nur noch die Möglichkeit der Löschung besteht. SWT ist der Ansicht, dass die Empfehlung «*praktisch nicht umsetzbar»* sei, *«da die bestehenden Profile keine Identitätsprüfung gemäss neuem Prozess durchlaufen haben und somit auch keine abgleichende Identitätsprüfung bei der Löschung des Profils erfolgen kann. Aus unserer Sicht könnte die Empfehlung 3 lediglich für Profile gemäss neuem Prozess erfolgen, weshalb wir diese Empfehlung ebenfalls als gegenstandslos betrachten*».

107 Der EDÖB teilt diese Haltung nicht. Aus dem Begleittext der Empfehlung (Ziff. 3.4) geht hervor, dass der Kern der Empfehlung die Verbesserung der Sicherheit bei der Änderung des Willens oder der Löschung von Profilen war. Die Tatsache, dass der Prozess von SWT nicht, wie ursprünglich geplant, angepasst wird, ändert jedoch nichts am Kern der Empfehlung. Der EDÖB ist der Ansicht, dass ein neuer Identifikationsprozess auch auf bestehende Profile angewendet werden könnte, ohne dass die Registrierung bereits nach diesem Prozess erfolgt sein muss.

108 Daraus folgt, dass der EDÖB die Empfehlung 3 von SWT als nicht angenommen erachtet. Dieser Punkt hat in Verbindung mit Empfehlung 2a zur Folge, dass es zwar nicht mehr möglich ist, einen bestehenden Registereintrag zu ändern. Allerdings ist es für die Nutzerinnen und Nutzer immer noch möglich, ihren Eintrag nach dem Einloggen in das Konto zu löschen. Da SWT weder die erhöhten Sicherheitsvorkehrungen für den Zugriff auf das Konto (Empfehlung 2a) noch die verstärkten Überprüfungen bei der Löschung des Kontos (Empfehlung 3) umsetzen wird, bleibt ein Restrisiko für eine unrechtmässige Löschung des Kontos – und damit des festgehaltenen Spendewillens – bestehen. Sollte es während der verbleibenden Zeit des Weiterbetriebs des NOSR zu unrechtmässigen Löschungen kommen, wird SWT unverzüglich reagieren und für bereits eingetretene Folgen entsprechender Missbräuche einstehen müssen.

109 Im Übrigen brachte SWT einige inhaltliche Anmerkungen an, die im vorliegenden Bericht aufgenommen worden sind.

5. Verfahren

5.1. Rechtliches Gehör und weiteres Vorgehen

110 Der EDÖB hat SWT am 17. Juni 2022 den vorliegenden Abschlussbericht samt Empfehlungen zur Prüfung und Stellungnahme vorgelegt. SWT wurde aufgefordert, innerhalb von 30 Tagen nach Erhalt zum Bericht Stellung zu nehmen und mitzuteilen, ob sie die Empfehlungen annimmt (vgl.

Ziff. 4). Der EDÖB kann dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art. 29 Abs. 4 DSG), soweit SWT die Empfehlungen ablehnt oder nicht befolgt.

111 Wie die in diesen Empfehlungen formulierten Vorgaben konkret umgesetzt werden, ist Sache von SWT. Im Rahmen der weiteren Zusammenarbeit und allfälligen Nachkontrollen wird der EDÖB entsprechende Umsetzungsvorschläge der Stiftung auf deren Datenschutzkonformität hin prüfen.

5.2. Veröffentlichung des Berichts und der Empfehlungen

112 Mit Blick auf die Bedeutung des NOSR besteht ein allgemeines Interesse daran, die Öffentlichkeit über die Feststellungen und Empfehlungen des EDÖB zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDÖB deshalb den vorliegenden Schlussbericht in angepasster Form und ohne namentliche Nennung von Mitarbeitenden der Beteiligten auf seiner Website (www.edoeb.admin.ch) veröffentlichen. Die Veröffentlichung des vollständigen Berichts steht unter dem Vorbehalt, dass aus Sicht der Stiftung keine vertraulichen Daten offengelegt werden, welche Geschäftsgeheimnisse preisgeben oder die Wettbewerbsfähigkeit beeinflussen könnten. SWT wurde deshalb aufgefordert, den Bericht auf solche vertraulichen Inhalte zu prüfen und gegenüber dem EDÖB innert derselben Frist von 30 Tagen schriftlich Stellung zu nehmen.

Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter

Adrian Lobsiger