Ostfalia
Hochschule für angewandte Wissenschaften

Richtlinie für die internationale Zusammenarbeit

Projekt „Digitales Vertrauen am Arbeitsplatz“

von Prof. Dr. Markus Launer

insbesondere für die internationale Datenverarbeitung

Projektleiter Prof. Dr. Markus Launer
Ostfalia Hochschule
Herbert-Meyer-Str. 7
29556 Suderburg
M-A.Launer@Ostfalia.de
Mobiltelefon 0177/6446410

Für den Bearbeitungszeitraum von Juli 2020 bis Juli 2023 (3 Jahre)

Überprüft und freigegeben
Datenschutzbeauftragte Prof. Dr. Klages, Ostfalia Hochschule
Kommission für Forschungsethik Ostfalia Hochschule

Inhalt

1 Präambel

Diese Richtlinie regelt die Datenverarbeitung für das Forschungsprojekt Digitales Vertrauen im Allgemeinen, für die Teilstudie DIGITAL TRUST @ the Workplace im Speziellen.

Das Anliegen dieser Richtlinie ist es, im Interesse der betroffenen Personen und auch des Projekts in jeder Phase der Informationsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten.

Um dieses Ziel zu erreichen, sind nicht nur gesetzliche Vorschriften zum Schutz personenbezogener Daten einzuhalten (siehe dazu gesonderte Regelungen unter https://www.ostfalia.de/cms/de/pws/launer/Forschung/digital-trust-at-the-workplace/), sondern auch geeignete technische und organisatorische Maßnahmen umzusetzen.

Alle Beteiligten müssen sich der Risiken bewusst sein, die mit technischen Systemen und Kommunikationstechnologien verbundenen sind, und bei der Verarbeitung personenbezogener Daten die erforderliche Sorgfalt walten lassen.

2 Grundsätzliches

Es gilt der Grundsatz der Datensparsamkeit und Datenvermeidung und damit die Reduzierung personenbezogener Daten auf ein notwendiges Minimum ("Datenvermeidung").

Zudem besteht eine Zweckbindung für die pseudonymen Daten ausschließlich für dieses Forschungsprojekt.

Für dieses Forschungsprojekt werden die pseudonym erhobenen Daten bestmöglich anonymisiert. Mithilfe von verschiedenen Maßnahmen werden personenbezogene Daten in einer Weise verändert, dass sie der konkreten Person nicht mehr zugeordnet werden können. Anonymisierung ist seit Einführung der DSGVO nicht mehr legal definiert. Die Definition aus dem § 3 Abs. 6 BDSG a.F. wird jedoch immer noch als Definitionshilfe herangezogen. Demnach versteht man unter anonymisieren „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

Die Anonymisierung der Daten des Forschungsprojektes erfolgt unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Deshalb treffen die Beteiligten geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. i. S. v. Art 32 Abs. 1 DSGVO.

Es werden alle möglichen technischen Vorkehrungen getroffen, um einen Verlust oder Diebstahl der Daten zu verhindern. Dazu wird ausschließlich auf gesondert gesicherten Computern gearbeitet.

3 Geltungsbereich sowie Projektverantwortung und -beteiligte

- Diese Richtlinie gilt persönlich für alle Wissenschaftler des Projekts, das sog. Digital Trust Team.
- Dazu gehören insbesondere der Projektverantwortliche Prof. Dr. Markus Launer (Ostfalia Hochschule) sowie Prof. Dr. Dave Marcial (Silliman University, Gastprofessor in 2020 an der Ostfalia Hochschule), Dr. Frithiof Svenson und Dierk Ohler (beides wissenschaftliche Mitarbeiter Ostfalia Hochschule).
- Dazu gehören alle involvierten Wissenschaftlicher, die an der Studie teilnehmen und diese Richtlinie unterschreiben oder im Auftrag von diesen arbeiten..
- Dazu gehört auch der Verantwortliche für die Datenverarbeitung i. S. d. DSGVO (siehe dazu die Vereinbarung über die Verarbeitung personenbezogener Daten gemäß Art. 13 DSGVO unter https://www.ostfalia.de/cms/de/pws/launer/Forschung/digital-trust-at-the-workplace/)
- Fragebogen der Studie: https://www.soscisurvey.de/digitaltrust/?r=mal

4 Anonymisierung der Daten

4.1 Erhebung und Umgang mit pseudonymen Daten

Bei diesem Forschungsprojekt müssen keine persönlichen Daten gelöscht oder pseudonymisiert werden. Die Daten liegen bereits in pseudonymer Form vor. „Pseudonymisierung“ ist nach Art. 4 DSGVO die Verarbeitung personenbezogener Daten in einer Weise, dass sich die personenbezogenen Daten nicht mehr einer spezifischen betroffenen Person zuordnen lassen, ohne zusätzliche Informationen hinzuzuziehen.

Es werden bei diesem Forschungsprojekt keine einzelnen Datensätze analysiert, verarbeitet oder veröffentlicht. Der Datensatz ist stets eine sehr große Menge an Daten.

Erhebung der Daten mittels des Fragebogens

Die Befragung im Rahmen des Forschungsprojekts “Digital Trust at the Workplace“ zielt nicht darauf, einzelne Personen zu identifizieren. Es werden keine eindeutigen Identifizierungskennzeichen erhoben wie Ihr Name und Ihre Anschrift. Es werden allein Ihre Angaben aus dem Fragebogen „Digital Trust at the Workplace“ verarbeitet. Dabei handelt es sich unter anderem um Alter, Geschlecht, Ausbildung, Familienstand, Geburtsland, Aufenthaltsland, Geburtsland, Erste Zahl der PLZ, Betriebszugehörigkeit etc.

Dabei kann es theoretisch möglich sein, dass mittels Kreuztabellierung eine Identifikation einer Person erfolgen könnte. Unser Ziel ist es, den Datensatz so gut wie möglich von potenziell identifizierenden Merkmalen zu bereinigen.

Die Notwendigkeit einer Aggregation von Informationen durch eine Vergröberung oder Aggregation von Informationen durch Bildung von Klassen oder Kategorien ist bereits im Fragebogen vorgesehen.

- Altersangaben sind durch Altersklassen ersetzt
- Konkrete Arbeitgeber werden nicht abgefragt, sondern lediglich die Angabe der Branche oder der Firmengrößenklasse
- Die Kategorie Ausbildung ist in möglichst grobe Kategorien aufgeteilt
- Die Kategorie Familienstand ist in möglichst grobe Kategorien aufgeteilt
- Die Kategorie Aufenthaltsland ist eine sehr grobe Einteilung nach Ländern
- Die Kategorie Geburtsland dient lediglich zur anonymen Identifikation von sog. Expatriates, d.h. im Ausland lebende Arbeitnehmer
- Die Kategorie Betriebszugehörigkeit ist in möglichst grobe Kategorien aufgeteilt

4.2 Keine formale Anonymisierung notwendig

Bei der formalen Anonymisierung werden direkte Identifizierungsmerkmale (Eigennamen von Personen und Orten, Bilder, Stimmen) aus den Forschungsdaten entfernt oder liegen von vornherein nicht vor. Bei diesem Forschungsprojekt bedarf es keiner formalen Anonymisierung, da keine direkten Identifizierungsmerkmale dem Ostfalia Team vorliegen. Lediglich die IP Adresse wäre ein Identifizierungsmerkmal. Diese verbleibt jedoch alleinig bei SoSci Survey GmbH für forensische Zwecke. Für das Ostfalia Team ist kein direkter Zugriff auf die IP möglich.

4.3 Durchführung der faktischen Anonymisierung

Die faktische Anonymisierung zielt darauf ab, die Daten so zu verändern, dass „die Person nur mit einem völlig unverhältnismäßigen Aufwand re-identifiziert werden kann“ (Metschke & Wellbrock 2002, S. 21).

4.3.1 Minderung des Re-Identifizierungsrisikos

Grundsätzlich ist bei der Einschätzung des Re-Identifikationsrisikos das „mögliche Zusatzwissen“ (Metschke & Wellbrock 2002, S. 21) der die Daten besitzenden Stelle bzw. eines potenziellen „Angreifers“ zu berücksichtigen. Dieses kann nicht nur aus den Forschungsdaten selbst, sondern auch aus sonstigen allgemein oder nicht allgemein zugänglichen Quellen stammen.

Ein Großteil der Daten wird über einen sog. Snowball-Effekt gesammelt. Die Befragenden leiten den Link zum elektronischen Fragebogen an Dritte weiter. Somit kennt auch der Befragende die Teilnehmer nicht mehr und kann diese auch nicht identifizieren. Somit könnte nur der direkt Befragende, aus dem pseudonymen Datensatz seine eigenen erhobenen Daten re-identifizieren. Keiner anderen Person ist es möglich, eine Person zu identifizieren, da der Teilnehmer an der Studie für diese völlig unbekannt ist. In diesem Projekt wird keiner der Befragenden eine Verteilerliste erstellen oder austauschen.

4.3.2 Vorab-Test auf Basis der Pre-Testdaten

Die indirekte, aber spezifische Kontextinformationen könnten zur Re-Identifizierung genutzt werden. Zu beachten sind Merkmalsausprägungen, die – in dem spezifischen Kontext – selten vorkommen. Der Fragebogen wurde vorab überprüft und auf sein Risiko hin untersucht.

Das Risiko einer Re-Identifikation aufgrund einer Kreuztabellierung ist als sehr gering einzustufen. Hierzu müssen alle Mittel berücksichtigt werden, die der Verantwortliche oder eine andere Person nach allgemeinem Ermessen wahrscheinlich nutzt, um die natürliche Person direkt oder indirekt zu identifizieren, beispielsweise das Aussondern. Hier spielen objektive Faktoren wie die Kosten der Identifizierung, der erforderliche Zeitaufwand, die verfügbare Technologie und technologische Entwicklungen eine Rolle.

Das Ostfalia Team hat auf Basis von über 350 Datensätzen aus dem Pre-Test einen Vorab-Test im Februar 2020 durchgeführt. Zwei Forscher haben unabhängig voneinander versucht, aus den pseudonymen Daten einzelne Personen zu analysieren. Die Primärforscher Prof. Dr. Dave Marcial (Silliman University) und Dierk Ohler (Ostfalia Hochschule) besitzen das größte Expertenwissen hinsichtlich der Forschungsdaten (vgl. Liebig et al. 2014). Sie können am besten die vorhandenen Re-Identifikationsrisiken sowie die Sensibilität der Daten einschätzen und die durch die Anonymisierung erreichten Eingriffe in das Analysepotenzial beurteilen. Auch bei der Wahl der Pseudonyme sind fachspezifische Kenntnisse erforderlich. Beide Forscher haben schriftlich bestätigt, dass aus dem Pre-Test keine Identifikation von personenbezogenen Daten möglich ist. Die Erfahrungen aus diesem Vorab-Test fließen nun die Anonymisierung des Datensatzes der Hauptstudie ein.

4.3.3 Best-mögliche Anonymisierung der Daten

Die Anonymisierung wird nach der Datensammlung zunächst von Dierk Ohler durchgeführt. Er selbst versendet keine Fragebögen und ihm sind daher keine einzelnen Personen bekannt, die an der Studie teilnehmen.

Ablauf der Anonymisierung

1. Identifikation der kritischen Daten(felder) bez. Datenfeldkombinationen
2. Prüfung ob nur wenig Datensätze zu einer Identifikation führen könnten
3. Wenige Datensätze lassen grundsätzlich keine Schlüsse im Rahmen einer wissenschaftlichen Arbeit zu, somit können die Datensätze entfernt oder in Datenpools überführt werden, die kein Rückschluss auf eine bestimmte Person zulassen

Bei der Anonymisierung werden die Datensätze markiert, die ein potentielles Re-Identifizierungsmerkmal haben könnten. Trotz der Vorkehrungsmaßnahmen im elektronischen Fragebogen werden u.a. folgende Überprüfungen angestellt:

- Kleine Gruppen unter 5 Personen je Kategorie werden in einer höheren Kategorie überführt (über 5 Personen per Kategorie)
- Mittels Kreuztabellierung wird versucht, einzelne Datensätze zu identifizieren

Es wird von Dierk Ohler ein Anonymisierungsprotokoll angefertigt, in dem alle Ersetzungen, Zusammenfassungen (Aggregationen) und Löschungen dokumentiert werden. Es wird dadurch auch festgehalten, welche Person/en die Anonymisierung durchgeführt haben. Das Anonymisierungsprotokoll und der Anonymisierungsschlüssel wird stets getrennt von den anonymisierten Dateien gespeichert und ist dem Ostfalia Team nicht zugänglich. Das Datenschutzprotokoll wird anschließend dem Datenschutzbeauftragtem der Ostfalia Hochschule zur Überprüfung zugesandt.

Es werden nur die anonymisierten Rohdaten aufbewahrt. Datensätze, die ein Risiko der Re-Identifizierung beinhalten, werden nach Stand der Technik unwiederherstellbar gelöscht. Eine Kopie der Originaldateien liegt somit nur bei der externen Firma SoSci Survey GmbH vor.

Den datenschutzrechtlich und forschungsethisch begründeten Ansprüchen an eine Anonymisierung der Daten im Interesse der Untersuchungspersonen stehen von Seiten der Forschung der Wunsch nach dem Erhalt von Informationen und der Sicherstellung des Analysepotenzials entgegen. Dieses Dilemma kann nur von Fall zu Fall, und zwar in Abhängigkeit vom konkreten Datenmaterial, den damit einhergehenden Schutzbedürfnissen der Betroffenen sowie den Interessen der Forschung, aufgelöst werden. Bei der Beurteilung der Risiken einer Re-Identifikation sind die potenziellen Schäden und Nachteile für die Untersuchungspersonen ebenso zu berücksichtigen wie die Wahrscheinlichkeit und die Komplexität eines Re-Identifizierungsversuchs durch einen „Angreifer“ (vgl. Häder 2009, S. 21).

4.4 Absolute Anonymisierung

Absolut anonymisierte Daten sind so verändert, dass die Re-Identifikation einer Person unmöglich ist (vgl. Medjedovic & Witzel 2010, S. 75ff.). Absolut anonymisierte Daten unterliegen damit nicht dem Datenschutz (vgl. Metschke & Wellbrock, 2002, S. 20).

Aggregierte Daten zum Zwecke der Anfertigungen von wissenschaftlichen Veröffentlichungen und Forschungspräsentationen auf Kongressen auf aggregierter Ebene unterliegen nicht dem Datenschutz. Die aggregierten Daten können daher problemlos untereinander ausgetauscht und veröffentlicht werden.

5 Übermittlung von Daten

Da es sich um eine globale Analyse handelt, werden Daten mit Forschern international geteilt. Empfänger der Daten sind die beteiligten Forscher an den nachfolgend genannten Universitäten, die das Ethikstatement und die Datenschutzerklärung anerkannt und diese Vereinbarung unterzeichnet haben.

Innerhalb der EU:

- Ostfalia Universität, Campus Suderburg, Deutschland (Leitung)
- SoSci Survey GmbH, Marianne-Brandt-Str. 29, 80807 München, Deutschland
- Linnaeus University, Schweden
- Tallinn University of Applied Sciences, Tallinn, Estland
- University of Coimbra, Portugal
- Babeș-Bolyai University, Rumänien
- Poznań University of Economics and Business, Polen
- Warsaw University of Life Science, Polen
- Slovak Academy of Sciences, Bratislava
- Linnaeus University, Kalmar, Sweden

Außerhalb der EU:

- University of Electro-Communication, Tokio, Japan
- Ferris University, Yokohama, Japan
- University Buenos Aires University, Argentinien
- Silliman University, Dumaguete, Philippines (Stellvertretende Leitung)
- Open University of the Philippines, Los Banos, Philippinen
- University of the Philippines, Manila, Cebu, Philippinen
- Shenzhen Polytechnic University, China
- Beijing Open University, Peking, China
- National Cheng Kung University, Tainan, Taiwan
- Semyung University, Semyung, Korea
- Siam University, Bangkok, Thailand
- Xavier School of Management - XLRI Jamshedpur, Indien
- Universidad Católica Nuestra Señora de la Asunción, Paraguay
- University de Chile, Santiago de Chile, Chile
- Bauman Moscow State Technical University, Russia
- University of Ghana Business School, Accra
- University of Nairobi, Kenia
- Faculdades Ibmec, Rio de Janeiro, Brasilien
- University of Oklahoma, Norman, USA
- Rider University, Lawrence Township, New Jersey, USA

In einigen der oben genannten Empfangsländer besteht aus Sicht der DSGVO kein angemessenes Datenschutzniveau. Voraussetzung für eine Datenübermittlung in diese Länder ist das Vorliegen angemessener Bestimmungen und Garantien für die Rechte und Freiheiten der betroffenen Personen (Unterzeichnung dieser Vereinbarung).

Die Daten werden nur auf sicherem Wege verschlüsselt übertragen. Dazu wird der Ostfalia Server „Powerfolder“ mit Passwort genutzt. Der datenaustausch wird somit per verschlüsseltem Download vollzogen. Es werden keine Daten per eMail übertragen, keine USB Sticks verwendet oder sonstige unsicheren Datenübertragungen. Lediglich aggregierte Daten zum Zwecke von Veröffentlichungen dürfen untereinander elektronisch ausgetauscht werden (vollständig anonymisiert und aggregiert).

6 Technische Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, werden geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

6.1 Datenschutz im Rahmen der laufenden Online-Umfrage

Die Daten werden während der Umfrage in der Cloud des Anbieters SoSci gesammelt. Dazu existiert ein Auftragsverarbeitungsvertrag (AVV) mit der SoSci Survey GmbH. Dabei werden systembedingt keine IP-Adressen gespeichert (es besteht also keine Zugriffsmöglichkeit auf

diese Information). Nach dem Ende der Umfrage werden die Daten beim Anbieter SoSci Survey GmbH unwiderruflich gelöscht.

Die Daten werden für die Verarbeitung durch das Ostfalia Team auf dem PowerFolder der Ostfalia Hochschule gespeichert. Der Zugang zu diesem PowerFolder ist nur mittels Einladung durch das Ostfalia Team (Projektleiter Prof. Launer) möglich. Zudem ist der PowerFolder Passwort-geschützt.

6.2 Zugangsbeschränkte Bereitstellung

Aufgrund des Restrisikos einer De-Anonymisierung wird der Schutz der pseudonymen Daten nicht nur mittels der Anonymisierung von Forschungsdaten gewährleistet, sondern diese mit weiteren Maßnahmen wie einer Zugangsbeschränkung kombiniert (vgl. z. B. Häder 2009 S. 21f.; Metschke & Wellbrock 2002, S. 22). Dies gilt insbesondere für internationale Reisen der beteiligten Forscher.

Die Bereitstellung der Daten für das Ostfalia und Digital Trust Team ist zugangsbeschränkt. Technisch werden die Daten nur auf vollverschlüsselten Computern gespeichert. Jeder Teilnehmer stellt sicher, dass dieser Computer nicht von Dritten genutzt werden kann. Er ist bei Nicht-Benutzung in einem Schrank abzuschließen. Nur Unterzeichner dieser Vereinbarung und dem Nachweis der ordnungsgemäßen Umsetzung erhalten Paßwort-geschützten Zugang.

6.3 Schutzmaßnahmen auf dem speziell präparierten Forscher-Notebook

Um den maximalen Schutz der Daten zu gewährleisten, werden einzelne Datensätze nur auf speziell präparierten Notebooks (im Folgenden als Forscher-Notebook bezeichnet) weiter verarbeitet. Zu diesem Zweck muss auf dem Forscher-Notebook die Software für die statistische Auswertung der Daten in der Sprache Englisch installiert sein. Weiterhin muss das Windows-System in die Sprache Englisch umschaltbar sein. Zur Grundausstattung des Notebooks gehören ein Virenscanner und eine Firewall.

Mit den Schutzmaßnahmen soll folgendes erreicht werden:

1. Verhinderung einer unberechtigten Nutzung
2. Erschwerte Einsichtnahme
3. Schutz vor Diebstahl

Schutzmaßnahme 1: Verschlüsslung der Speichermedien im Forscher-Notebook

Für das Forscher-Notebook wird Windows 10 verwendet. Als erste Schutzmaßnahme werden alle integrierten Datenträger (Festplatte usw.) mit der in Windows 10 integrierten Technologie Bitlocker mit einem 256-Bit AES-Schlüssel verschlüsselt (Festplattenver-schlüsselung). Der Schlüssel ist nur in den Händen des Digital Trust Teams des Projektes. Somit sind die Daten auf dem Forscher-Notebook ohne Eingabe des Schlüssels nicht zugänglich. Ein Auslesen im Live-Betrieb (bei geöffneten Notebook-Gehäuse) verhindert das Trusted Platform Module (TPM), das in handelsüblichen Notebooks eingebaut ist.

Schutzmaßnahme 2: Verhinderung von unerlaubten Blicken und entfernten Kameraaufnahmen

Um visuelles Hacking durch verstohlene Blicke von der Seite auf den Bildschirm zu vermeiden und entfernte Kameraaufnahmen zu verhindern, wird eine Blickschutzfolie (Beispiel von 3M) einsetzt.

Schutzmaßnahme 3: Verhinderung von physischem Diebstahl

Nachts wird das Gerät verschlossen aufbewahrt oder im Safe des jeweiligen Hotels (auf Reisen). Im laufenden Betrieb, wenn das Gerät vorübergehend ohne Aufsicht ist, wird das Forscher-Notebook z- B- mit einem Kensington-Schloss (Beispiel: Kensington MiniSaver, Kensington K64637WW ClickSafe) vor Ort an einen möglichst schweren Arbeitstisch „angekettet“. Damit wird ein physischer Diebstahl erschwert bzw. verhindert.

6.4 Datenschutz im Rahmen der Archivierung

Die einzelnen Datendateien werden auf der (Ostfalia) Powerfolder als verschlüsselte ZIP-Datei im Rahmen des festgelegten Zeitraums zur Archivierung abgelegt. Dabei wird die ZIP-Datei zusätzlich mit Gpg4Win (vom Bundesamt für Sicherheit in der Informationstechnik, Kürzel BSI empfohlen) verschlüsselt.

6.5 Übersicht der Szenarios und technischen Maßnahmen

Szenario	Verhinderung durch Schutzmaßnahme
Versuch des **Datendiebstahls** im laufenden Betrieb **mit Aufsicht**	▪ Blickschutzfolie
Versuch des **Datendiebstahls** im laufenden Betrieb **ohne Aufsicht**	▪ Blickschutzfolie ▪ Portsperre (Datenaustausch unmöglich)
Physischer Diebstahl des Forscher-Notebooks im **laufenden Betrieb**	▪ Kensington Schloss ▪ TPM (bei Öffnung des Geräts) ▪ Luggage Tracker (optional)
Physischer Diebstahl des Forscher-Notebooks bei einem **Raubüberfall**	▪ Festplattenverschlüsslung (mit Passwort) ▪ Standart-Passwortschutz und Portsperre ▪ Luggage Tracker (optional)
Physischer Diebstahl des Forscher-Notebooks im **Reisegepäck** oder Hotelsafe	▪ Festplattenverschlüsslung (mit Passwort) ▪ Standart-Passwortschutz und Portsperre ▪ Luggage Tracker (optional)

7 Zusätzliche Datenschutzbestimmungen

7.1 Datenschutzvorfälle

- Bei der Verletzung des Schutzes personenbezogener Daten, etwa durch Abfluss von Daten nach einem IT-Vorfall oder durch unbefugten Zugriff auf Daten nach dem Verlust eines Notebooks, ist innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde für den Datenschutz abzusetzen. Soweit die Voraussetzungen des Art. 34 DSGVO erfüllt sind, müssen auch die von der Verletzung Betroffenen benachrichtigt werden.
- Vor der Meldung an die Aufsichtsbehörde und der Benachrichtigung der Betroffenen ist der DSB anzuhören. Der Inhalt von Meldung und Benachrichtigung ist mit ihm abzustimmen.
- Die Abteilung des Unternehmens, in deren Verantwortungsbereich der Datenschutzvorfall fällt, schlägt unverzüglich Maßnahmen zur Behebung der Verletzung und zur Abmilderung möglicher nachteiliger Auswirkungen vor. Soweit Maßnahmen keinen Aufschub dulden, sind sie umgehend zu ergreifen. Sämtliche Maßnahmen werden dokumentiert.
- Wenn von einer Meldung abgesehen werden kann, sind die Gründe dafür gemäß Art. 33 Abs. 5 DSGVO zu dokumentieren.

7.2 Sensibilisierung

- Forscher, die an den Verarbeitungsvorgängen beteiligt sind, werden in geeigneter Weise für den Datenschutz sensibilisiert.
- Zudem sind alle beteiligten Forscher an das Ethikstatement gebunden, dass von der Kommission für Forschungsethik der Ostfalia Hochschule (https://www.ostfalia.de/cms/de/pws/launer/Forschung/digital-trust-at-the-workplace/) festgelegt wurde. Weitere detaillierte Angaben der Kommission für Forschungsethik finden Sie auf der Internetseite der Hochschule unter https://www.ostfalia.de/cms/de/forschung/kommission-fuer-forschungsethik/index.html.

7.3 Vertraulichkeit

- Den beteiligten Forschern ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Sie sind vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit schriftlich zu verpflichten. Die Verpflichtung erfolgt durch den Projektverantwortlichen unter besonderem Hinweis auf die strafrechtlichen Vorschriften des Datenschutzrechts.

8 Veröffentlichungen und Teilnahme an Konferenzen

Die Forscher, die auf Basis der gesammelten Daten Veröffentlichungen anfertigen und an Konferenzen teilnehmen, verpflichten sich

- Auf Basis der Theorien von Prof. Dave Marcial und Prof. Dr. Markus Launer zu arbeiten und diese zu zitieren
- Prof. Dr. Markus Launer an dallen Veröffentlichungen zu beteiligen und bei allen Veröffentlichungen als Co-Autor anzugeben.

9 Einverständniserklärung

_____

Projektverantwortlicher: Name, Vorname, Universität, Adresse

_____

Mitarbeiter, Statistiker: Name, Vorname, Universität, Adresse

_____

Externe Dienstleister: Name, Vorname, Universität, Adresse