Praktischer Datenschutz im Alltag:

- Unbefugten den Zugriff auf pbDaten (personenbezogene Daten) stets verweigern
- Unterlagen mit pbDaten nicht sichtbar liegen lassen (mindestens „Face down“ ablegen)
- Bürotür bei leerem Büro nie unverschlossen lassen (ist die einzige Barriere zur Außenwelt)
- Auch bei kurzer Abwesenheit den Bildschirm sperren (z.B. mit Tastenfolge [Win] + L)
- Zur Entsorgung von Unterlagen mit pbDaten nur die Entsorgungstonnen (Silbertonnen) oder geeignete Aktenvernichter (Sicherheitsstufe P3) verwenden
- Keine Auskünfte über pbDaten erteilen, ohne vorher die Berechtigung der anfragenden Stelle positiv überprüft zu haben
- Vertrauliche Informationen (pbDaten) nicht unverschlüsselt per E-Mail versenden
- Bei Versand von E-Mails an Gruppen, die „bcc“-Funktion benutzen
- „Datenpannen“, d.h. Verlust, unbeabsichtigte Veröffentlichung oder Verfälschung von pbDaten umgehend der/dem Vorgesetzten und dem bDSB melden
- Externe Cloud-Dienste dürfen zur Verarbeitung von pbDaten nur genutzt werden, wenn zwischen dem Dienstanbieter und der UW/H gGmbH ein Auftragsverhältnis besteht (AV-Vertrag)

Wichtig: „Pseudonym“ ist nicht „Anonym“

Auch wenn ein Personenbezug in Daten nur indirekt, z.B. über ein Pseudonym und eine zusätzliche Zuordnungstabelle möglich ist, handelt es sich um personenbezogene Daten. Alle Vorschriften aus der DSGVO gelten auch für pseudonyme pbDaten.

Alle Bereiche der UW/H sind in der Pflicht

Die gesetzlichen Datenschutzpflichten müssen bei jeder Verarbeitung von pbDaten (personenbezogenen Daten) beachtet werden, egal, ob die Verarbeitung etwa für Zwecke der Verwaltung oder für Zwecke der Forschung/Lehre oder für Zwecke der Patienten-versorgung erfolgt.

Weitere Informationen im Intranet

Zum Datenschutz an der UW/H finden Sie weitere Hinweise auf der Intranet-Seite des betrieblichen Datenschutzbeauftragten (bDSB):

https:/
/intranet.uni-wh.de
/arbeiten
/administrationseinheiten-a-z
/beauftragte-stabsstellen
/datenschutzbeauftragter

Oder einfach das Stichwort „Datenschutzbeauftragter“ in die Seitensuche eingeben.

Kontakt zum bDSB der UW/H

Den betrieblichen Datenschutzbeauftragten der UW/H erreichen Sie via Briefpost / Hauspost am Standort Witten: Alfred-Herrhausen-Straße 50,

oder telefonisch unter 02302 / 926 – 722.

Der einfachste Weg ist aber eine E-Mail an:

datenschutz@uni-wh.de

Versionshinweis:
Handzettel Datenschutz (Stand 2023-08-31).docx
Autor: Martin Rützler (bDSB der UW/H)

universität Witten/Herdecke

DATENSCHUTZ an der UW/H gGmbH

Ein Kurz-Wegweiser für die Büro-Pinnwand

Datenschutz ist ein Grundrecht und
schützt Menschen bei der Verarbeitung ihrer Daten

EU-Grundrechtecharta
Art. 8 - Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

https://www.europarl.europa.eu/charter

Verarbeitungen von personenbezogenen Daten (pbDaten) an der UW/H sind nur dann datenschutzfreundlich, wenn sie:

1. ausschließlich auf Basis einer zugelassenen Rechtsgrundlage (RGL) erfolgen; es gilt das Prinzip „Verbot mit Erlaubnisvorbehalt“
    - RGL für „normale“ pbDaten: Art. 6 DSGVO*
    - RGL für „besondere“ pbDaten: Art. 9 DSGVO*,

2. die Grundsätze aus Art. 5 DSGVO* erfüllen (dazu zählen u.a. Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit),

3. unter Anwendung ausreichender Maßnahmen (technisch und organisatorisch) zur Gewährleistung einer angemessenen IT-Sicherheit erfolgen (Artt. 25, 32 DSGVO*),

4. transparent für die von der Verarbeitung ihrer Daten betroffenen Personen sind, d.h.
    - Vorab-Information gemäß Artt. 13, 14 DSGVO*
    - Beantwortung von Auskunftsanfragen gemäß Art. 15 DSGVO* sowie sonstiger Betroffenenrechte
    - Information über Datenpannen, die ein hohes Risiko für die betroffenen Personen auslösen (Art. 34 DSGVO*),

5. im zentralen Verzeichnis von Verarbeitungstätigkeiten (VVT) der UW/H dokumentiert sind (Art. 30 DSGVO*).

(*) https://datenschutz-wiki.de/Datenschutz-Grundverordnung

Die Datenschutzgesetze:

DSGVO (Europa)

Die „Datenschutz-Grundverordnung“ schreibt für alle EU-Mitgliedsstaaten einheitliche und gemeinsame Regeln für den Umgang mit pbDaten vor. Dadurch wird ein gleiches Datenschutzniveau in ganz Europa sichergestellt.

Vor Übermittlungen von pbDaten in Länder außerhalb der EU muss geprüft werden, ob in diesen „Drittländern“ ein gleichwertiges Datenschutzniveau gewährleistet wird. Falls nicht, sind zusätzliche Sicherungsmaßnahmen erforderlich.

BDSG (Deutschland)

Das „Bundesdatenschutzgesetz“ konkretisiert die DSGVO-Vorgaben für die Anwendung in Deutschland. Die EU-Grundverordnung lässt jedoch nur noch enge Spielräume. So ist die DSGVO auch in Deutschland das wesentliche Regelwerk für alle Datenschutzfragen.

LDSG (NRW)

Das „Landesdatenschutzgesetz NRW“ regelt die Umsetzung der DSGVO-Anforderungen für die öffentlichen Stellen (z.B. Behörden) in Nordrhein-Westfalen.

Unabhängige Stelle zur Datenschutzaufsicht

Überwachende Stelle für alle privaten und öffentlichen Organisationen in NRW ist die:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4, 40213 Düsseldorf
Telefon: 0211/38424-0
E-Mail: poststelle@ldi.nrw.de

Spezialfälle bei der Verarbeitung von pbDaten:

Die Person oder Stelle, die die Zwecke (Wozu?) und die Mittel (Womit?) einer Verarbeitung von pbDaten bestimmen kann, trägt die datenschutzrechtliche Verantwortung für die Verarbeitungstätigkeit. Sie wird als „Verarbeitungsverantwortliche:r (VV)“ bezeichnet.

Sind neben der/dem VV an der Verarbeitung weitere Personen oder Stellen beteiligt, muss geklärt werden, wie sich das auf die datenschutzrechtliche Verantwortung auswirkt.

Es gibt neben der Alleinverantwortung zwei weitere Modelle:

1. Auftragsverarbeitung (Art. 28 DSGVO)
   Hierbei lagert die/der VV mehr oder weniger große Teile der Gesamtverarbeitung an eine externe Stelle aus. Dieser „Auftragsverarbeiter (AV)“ darf die pbDaten nur weisungsgebunden (d.h. nicht zu eigenen Zwecken) verarbeiten. Die Gesamtverantwortung bleibt beim VV. Der AV muss jedoch eine ausreichende IT-Sicherheit auf seiner Seite gewährleisten können.

2. Gemeinsame Verantwortlichkeit (Art. 26 DSGVO)
   Legen zwei oder mehr Stellen die Zwecke und Mittel einer Verarbeitung gemeinsam fest, tragen sie die datenschutzrechtliche Verantwortung gemeinsam. Es muss in einer Vereinbarung geklärt werden, welche Stelle welche Pflichten aus der DSGVO übernimmt.

In beiden Fällen müssen entsprechende Verträge (AV-Vertrag, GV-Vertrag) abgeschlossen werden.