Blum&Grob
RECHTSANWÄLTE

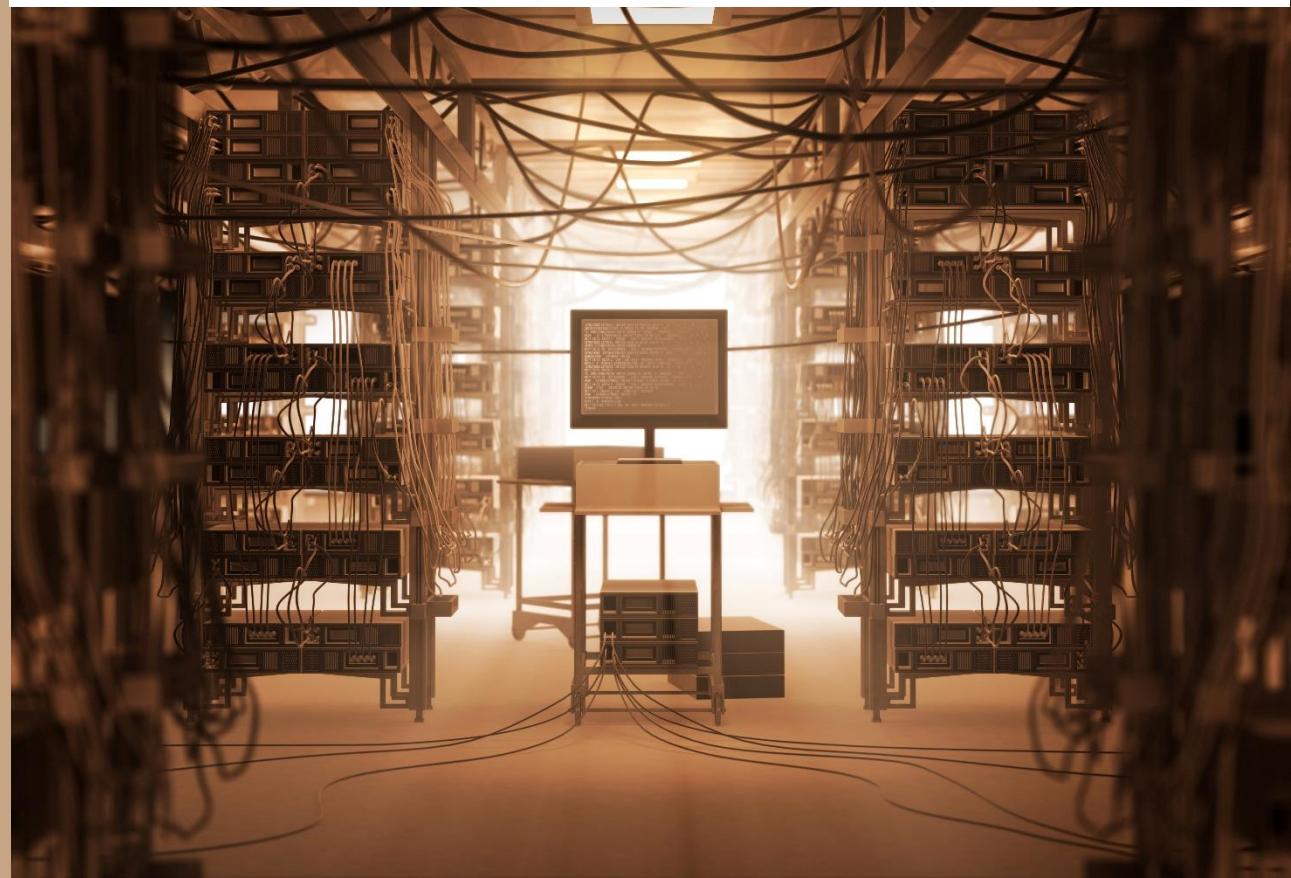
Zurich University
of Applied Sciences

zh
aw

Life Sciences and
Facility Management

Institute of
Facility Management

IFMA™ Switzerland Chapter
International Facility Management Association



Das neue Datenschutzgesetz – Was kommt auf das FM zu?

9 Schritte zur Umsetzung

Blum&Grob | Zürich, Juli 2023

Moderation

Dr. Simon Ashworth, Mitarbeiter am IFM der ZHAW, Moderation

- Forschungsschwerpunkt BIM und andere Digitalisierungsthemen in Bezug auf Immobilien und FM
- Mehr als 20 Jahre praktische FM-Erfahrung aus den Unternehmen Serco sowie der britischen Verteidigungsakademie
- Seine Forschungsergebnisse sind unter Researchgate frei verfügbar

Referenten

David Schwaninger
d.schwaninger@blumgrob.ch

Dr. Giedre Neverauskas
g.neverauskas@blumgrob.ch

Revision DSG
Ausgangslage

Wieso ist Datenschutz wichtig?

Was bisher geschah

- Am 1. September 2023 tritt das vollständig revidierte Datenschutzgesetz (revDSG) und die revidierte Datenschutzverordnung (revDSV) in Kraft, ohne Übergangsfrist
- Die Schweiz holt im Datenschutz gegenüber der EU auf
  - Grundsatzbasiert, nicht so detailliert wie die DSGVO
  - Angemessenheitsentscheid ausstehend
- Aber: Keine grundlegende Änderung des Grundkonzepts
  - Bisher erlaubte Bearbeitungstätigkeiten können grundsätzlich weitergeführt werden
  - Keine Kopie der EU-Datenschutzgrundverordnung (DSGVO), viele Regelungen werden aber übernommen
  - Governance und Rechte der Betroffenen werden erweitert

Datenbegriff: Daten nach revDSG

- Geltung für Bund und Private (nicht Kantone)
- Nur Personendaten (bestimmt oder bestimmbar)
- Daten von natürlichen und juristischen Personen (noch…)
- Ausnahme: anonymisierte oder pseudonymisierte Daten
- Inhaltlich: Bearbeitung von Personendaten, sprich jeder Umgang mit Personendaten

(Ausnahme: Bearbeitung ausschliesslich zum persönlichen Gebrauch)

Datenschutz betrifft künftig nur Daten über natürliche Personen

Besonders schützenswerte Personendaten

Religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten

Gesundheit, Intimsphäre, Rassen-/Ethnienzugehörigkeit

Massnahmen der sozialen Hilfe

Administrative oder strafrechtliche Verfolgungen und Sanktionen

Künftig auch genetische und biometrische Daten

Profiling

«Auswertung von automatisiert bearbeiteten Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen.»

*Profiling **mit hohem Risiko**: eine Verknüpfung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.*

Vereinzelt von Relevanz

&

Weitere wichtige Definitionen

- **Bearbeiten:** jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
  - Grundsätzlich ist keine Rechtsgrundlage erforderlich; nur falls die Grundsätze nicht beachtet werden, wenn besonders schützenswerte Daten an Dritte weitergegeben werden oder wenn die betroffene Person widerspricht
  - Einwilligung nur in Einzelfällen notwendig (z.B. bei besonders schützenswerten Personendaten)

- **Verantwortlicher**: Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

- **Auftragsbearbeiter**: Person, die im Auftrag des Verantwortlichen Personendaten bearbeitet.

Einwilligung

- Muss **freiwillig** und in Kenntnis der Sachlage abgegeben werden
- Kästchen können vorangekreuzt werden, wenn das Formular die Schaltfläche "Annahme" enthält
- Kann in einen Vertrag aufgenommen werden, wenn ein sachlicher Zusammenhang besteht
- Keine Information über das Widerrufsrecht erforderlich
- Der Widerruf kann in bestimmten Situationen eingeschränkt sein (z. B. im Zusammenhang mit Kosten)
- **Ein Muss bei besonders schützenswerten Personendaten & Profiling mit hohem Risiko**

&

Strafsanktionen

- Die Eidgenössische Datenschutzbehörde (EDÖB) kann
  - Bearbeitungstätigkeiten untersuchen
  - Anordnungen zur Einschränkung, Änderung oder Einstellung von Bearbeitungstätigkeiten erlassen
- Die kantonalen Behörden können
  - Bei vorsätzlicher Verletzung von Bestimmungen des revDSG oder bei unterlassener Zusammenarbeit mit der Datenschutzbehörde, Bussen bis zu CHF 250'000 gegen Einzelpersonen aussprechen
  - Sanktionen gegen Verwaltungsrat gemäss Art. 6 und 7 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR)
  - Keine Versicherung/Entschädigung

Die Bussen betreffen die Verantwortlichen persönlich

Revision DSG
9 Schritte zur Umsetzung

Vorgehen

Unser Framework
Vorgehensmodell

Kick-Off

- Detaillierte Abstimmung Vorgehen und Termine
- Vorstellen Ergebnisse der Desktop Analyse
- Planung der Interviews

Situationsanalyse

- Fragenkatalog
- Analyse Prozesse
- Analyse Systeme & Datenflüsse

Beurteilung & Identifikation GAPs

- Abgleichen der Situationsanalyse mit den Anforderungen des DSG
- Erstellen des Inventars der identifizierten GAPs

Massnahmenplanung

- Ableiten von Massnahmen zur Schliessung der GAPs
- Schlussbesprechung und Bericht

Schritt 1: Bearbeitungsverzeichnis erstellen

Bearbeitungsverzeichnis für KMU oft nicht notwendig (weniger als 250 FTE)

Schritt 1: Bearbeitungsverzeichnis erstellen

- Inventar der Bearbeitungstätigkeiten des Verantwortlichen oder Auftragsbearbeiter (beide führen je ein separates Verzeichnis)

- **KEINE** Pflicht bei Unternehmer mit weniger als 250 Angestellten, es sei denn,
  - Bearbeitung besonders schützenswerter Personendaten in grossem Umfang und/oder
  - Profiling mit hohem Risiko

- **Keine Sanktion**
- **Vorteil: Analyse der Datenbearbeitungen / IT-Anbieter; Optimierungsmöglichkeiten**

Schritt 1: Bearbeitungsverzeichnis erstellen

Inhalt gemäss Art. 12 Abs. 2 revDSG:

Identität Verantwortlicher	Bearbeitungszweck	Kategorie betroffener Personen	Kategorien bearbeiteter Personendaten	Kategorie der Empfänger	Aufbewahrungsdauer	Massnahmen Datensicherheit	Auslandsübermittlung: Staat und Garantien

Schritt 2: Datenschutzerklärung aktualisieren

Datenschutzerklärung vorhanden?
Aktualisierung notwendig?

Schritt 2: Datenschutzerklärung aktualisieren

- Obligatorische Informationspflicht bei **jeder** Datenbeschaffung
  - Vertragspartner
  - Mitarbeiter
- Minimuminhalt gesetzlich definiert (Art. 19 Abs. 2 revDSG)
  - Identität und Kontaktdaten des Verantwortlichen
  - Bearbeitungszweck
  - Empfänger bzw. Empfängerkategorie
  - Insbesondere muss Liste der Länder enthalten sein, in welche Personendaten übermittelt werden und ggf. Garantien, wenn kein adäquater Datenschutz
  - Automatisierte Einzelentscheidung.
- **Sanktion bis zu CHF 250’000.00**
- **Kostenersparnis: weniger Auskunftsanfragen → weniger admin. Aufwand**

Schritt 3: Vertrag mit Auftragsbearbeiter überprüfen

Verträge betreffend Auftragsbearbeitung überprüfen

Schritt 3: Vertrag mit Auftragsbearbeiter überprüfen

- Wenn die Bearbeitung von Personendaten an einen Auftragsbearbeiter delegiert wird, muss ein Vertrag abgeschlossen werden, welcher folgende Punkte enthält:
  - Weisungsrecht, Aufsicht, Beistandspflicht
  - Gewährleistung der Datensicherheit
  - Einsatz von Unterauftragsbearbeiter nur mit Zustimmung des Verantwortlichen (neu)

- Aber: Ein Auftragsbearbeiter wird zum Verantwortlichen, wenn er Personendaten für eigene Zwecke verwendet oder wesentliche Aspekte der Bearbeitung bestimmt
  - Auch in solchen Situationen sollte ein Vertrag abgeschlossen werden

- **Sanktion bis zu CHF 250’000.00**
- **Vorteil: Inventar der IT-Anbieter; Optimierungsmöglichkeiten**

Schritt 4: Datenübermittlungen ins Ausland überprüfen

Gibt es Datenübermittlungen ins Ausland?
Falls ja, in welche Länder?
Welche Garantien werden eingesetzt?

Schritt 4: Datenübermittlungen ins Ausland überprüfen

- Personendaten dürfen nur ins Ausland übermittelt werden, wenn der Empfängerstaat ein angemessenes Schutzniveau hat (Art. 16 Abs. 1 revDSG)

- Fehlt ein solches Schutz (z.B. USA, China, Indien), müssen Garantien vorliegen (Risikobasierter Ansatz)
  - Völkerrechtlicher Vertrag (Art. 16 Abs. 2 lit. a revDSG)
  - Datenschutzklausel in einem Vertrag (vorherige Mitteilung an EDÖB)
  - Weitere risikobasierte Garantien (vorherige Mitteilung an EDÖB);
  - Vom EDÖB genehmigte SCC oder Binding Corporate Rules

- **Sanktion bis zu CHF 250’000.00**

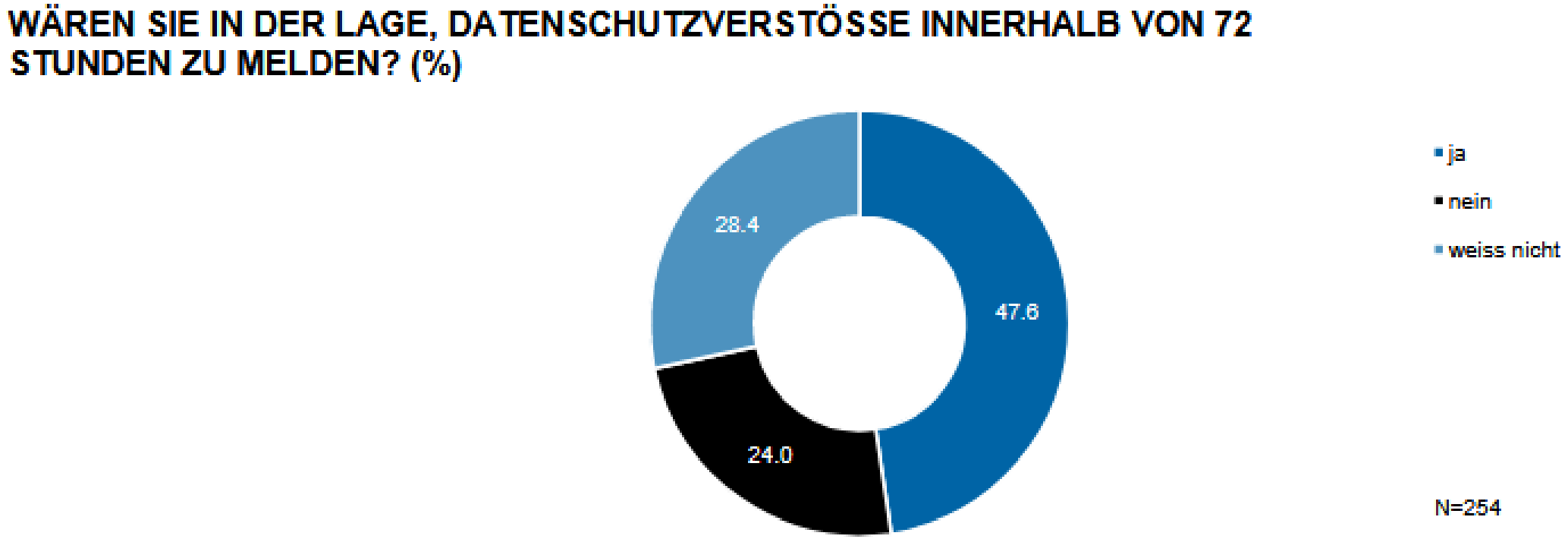
Schritt 5: Prozess betreffend Data Breach definieren

Besteht ein Konzept betreffend Data Breach?
Aktualisierung notwendig?

Schritt 5: Prozess betreffend Data Breach definieren

- Datenschutzverletzung: ungeplante Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten
  - Beispiele: Falsch versandte Mails, Datenverlust, Hackerzugriffe
- Meldung an den EDÖB nur, wenn ein "hohes Risiko" negativer Folgen für die betroffenen Personen besteht
  - Meldung («so rasch als möglich»), sobald die vorgeschriebenen Informationen vorhanden sind
  - Aber: Zuwiderhandlung wird nicht sanktioniert
- Muss auch der betroffenen Person mitgeteilt werden, wenn dies zu ihrem Schutz erforderlich ist (z.B. Änderung des Passworts).
- Auch die Auftragsbearbeiter müssen alle Datenverletzungen melden
- **Keine Sanktion**

Beispiel – Datensicherheit



Quelle: Datenschutz in Schweizer Unternehmen 2018, Studie des Instituts für Wirtschaftsinformatik und des Zentrums für Sozialrecht der ZHAW

Können Sie die Vorgaben einhalten?

Schritt 6: Etablierung von technischen und organisatorischen Massnahmen

Was für technische und organisatorische Massnahmen werden zurzeit eingesetzt?

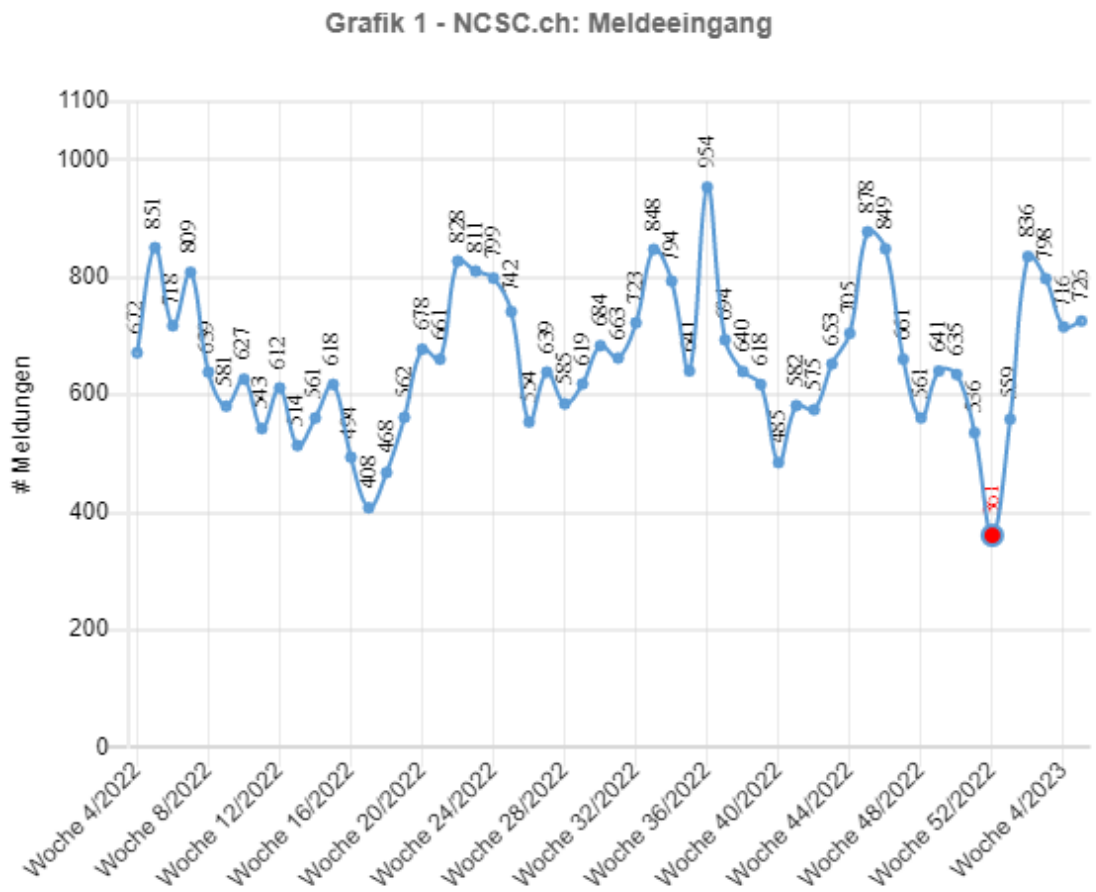
Schritt 6: Etablierung von technischen und organisatorischen Massnahmen

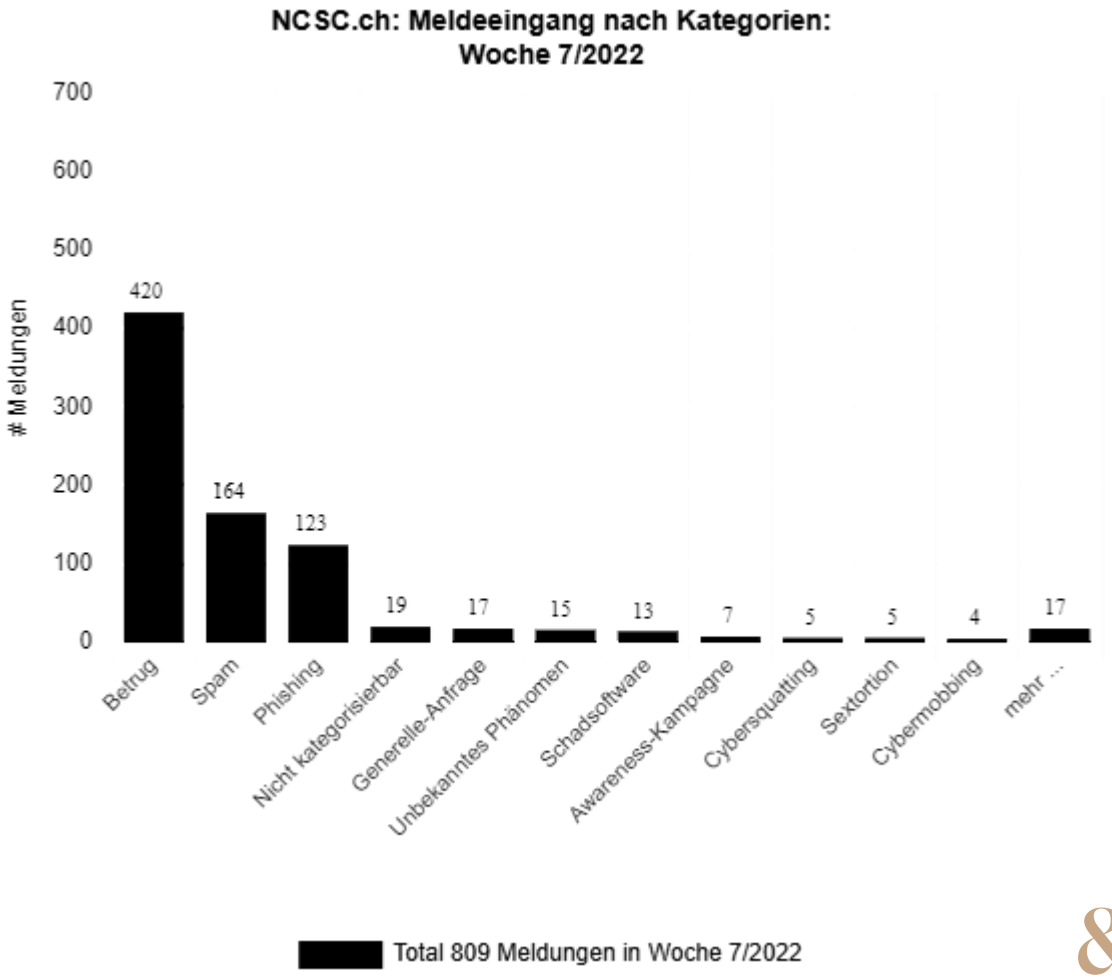
- **Vertraulichkeit, Integrität, Verfügbarkeit** (Ausreichend & den Risiken angemessen)
- **Privacy by Design**
  - Anonymisierung
  - Datenminimierung
  - Datentrennung nach Zweck
  - Löschkonzept
- **Privacy by Default**

  Standardmässig müssen die Datenschutzeinstellungen des Endnutzers auf die am wenigsten invasive Option eingestellt sein
- **Sanktion bis zu CHF 250’000.00**
- **Vorteil: datenschutzrechtliche Vorgaben in den Systemen integriert, spart nachträglichen Aufwand**

&

Be*un*ruhigender Trend
Die Anzahl von Cyberangriffen wächst





Quelle: https://www.ncsc.admin.ch/ncsc/de/home.html

Schritt 7: Erstellen/Überarbeiten von Musterkorrespondenz betreffend Betroffenenrechte

Wie werden heute Betroffenenrechte umgesetzt?

Schritt 7: Erstellen/Überarbeiten von Musterkorrespondenz betreffend Betroffenenrechte

- Auskunft über ihre Daten, Berichtigung, Widerspruch gegen die Bearbeitung bzw. Löschung/Anonymisierung, Datenherausgabe- oder -übertragung
  - Diese Rechte sind keine absoluten Rechte; sie können von dem für die Bearbeitung Verantwortlichen aus bestimmten Gründen eingeschränkt werden (z. B. bei bestimmten überwiegenden Interessen)
  - Die Rechte der betroffenen Person sind in der Regel unentgeltlich
  - Ordnungsgemässe Identifizierung des Antragstellers

- Neuer besserer Schutz gegen missbräuchliche Auskunftsersuchen
  - Beantwortung innerhalb von 30 Tagen, keine Notwendigkeit der Bestätigung der "Vollständigkeit«

- **Sanktion bis zu CHF 250’000.00**

Schritt 8: Prozess betreffend Datenschutz-Folgenabschätzung etablieren

Um hohe Risiken für Persönlichkeitsrechte zu erkennen & zwecks Feststellung des Bedarfs für Datenschutz-Folgenabschätzung

Schritt 8: Prozess betreffend Datenschutz-Folgenabschätzung etablieren

- **Voraussetzung**: ein **hohes Risiko** einer **Verletzung der Persönlichkeit** oder der **Grundrechte** einer betroffenen Person durch eine beabsichtigte Datenbearbeitung
  - Umfangreichen Bearbeitung besonders schützenswerter Personendaten (z.B. Gesundheitsdaten, biometrische Daten, Konfession, Strafsanktionen, etc.);
  - Wird systematisch umfangreiche öffentliche Bereiche überwacht werden
  - Andere Fälle (grosse Mengen, Zugriffsmöglichkeit für hohe Anzahl von Personen, etc.)

- **Keine Sanktion**
- **Vorteil: EDÖB erwartet, dass hohe Risiken analysiert & Massnahmen ergriffen werden; Risikoausschluss nicht zwingend nötig**

Schritt 9: Schulung der Mitarbeiter

Mitarbeiter schulen und Verantwortlichkeiten festlegen

Schritt 9: Schulung der Mitarbeiter

- Ohne entsprechende Anweisungen wissen die Mitarbeiter nicht, was sie tun müssen und dürfen
  - Anweisungen und Anleitungen müssen rechtzeitig angepasst werden
  - Vorlagen, Formulare und Checklisten müssen erstellt werden
  - Schulungen sollen durchgeführt und Anwesenheit protokolliert werden
  - Die Einhaltung des Datenschutzgesetzes soll dokumentiert werden, insbesondere für den Fall, dass ein Verfahren eingeleitet wird

- Aber: Ein "Datenschutzberater" ist nicht zwingend erforderlich

Was können wir für Sie tun?

Individuelle und effiziente Umsetzung der Vorgaben:

Prüfung, Beratung und Erstellung
Datenschutzerklärungen und -richtlinien
Bearbeitungsverzeichnis
Verträge mit Auftragsdatenbearbeiter:innen
Datenübermittlungen ins Ausland
Datenschutzfolgenabschätzung
Analyse, Beratung und Etablierung
Data Breach-Prozess
Technische und organisatorische Massnahmen
Umsetzung der Betroffenenrechte
Schulung
Schulung von Key-Mitarbeitern

Kontakt

Blum & Grob Rechtsanwälte AG
Neumühlequai 6
Postfach
CH – 8021 Zürich

T +41 58 320 00 00
F +41 58 320 00 01
d.schwaninger@blumgrob.ch
g.neverauskas@blumgrob.ch