Die Wohnungswirtschaft
Norddeutschland, Niedersachsen und Bremen

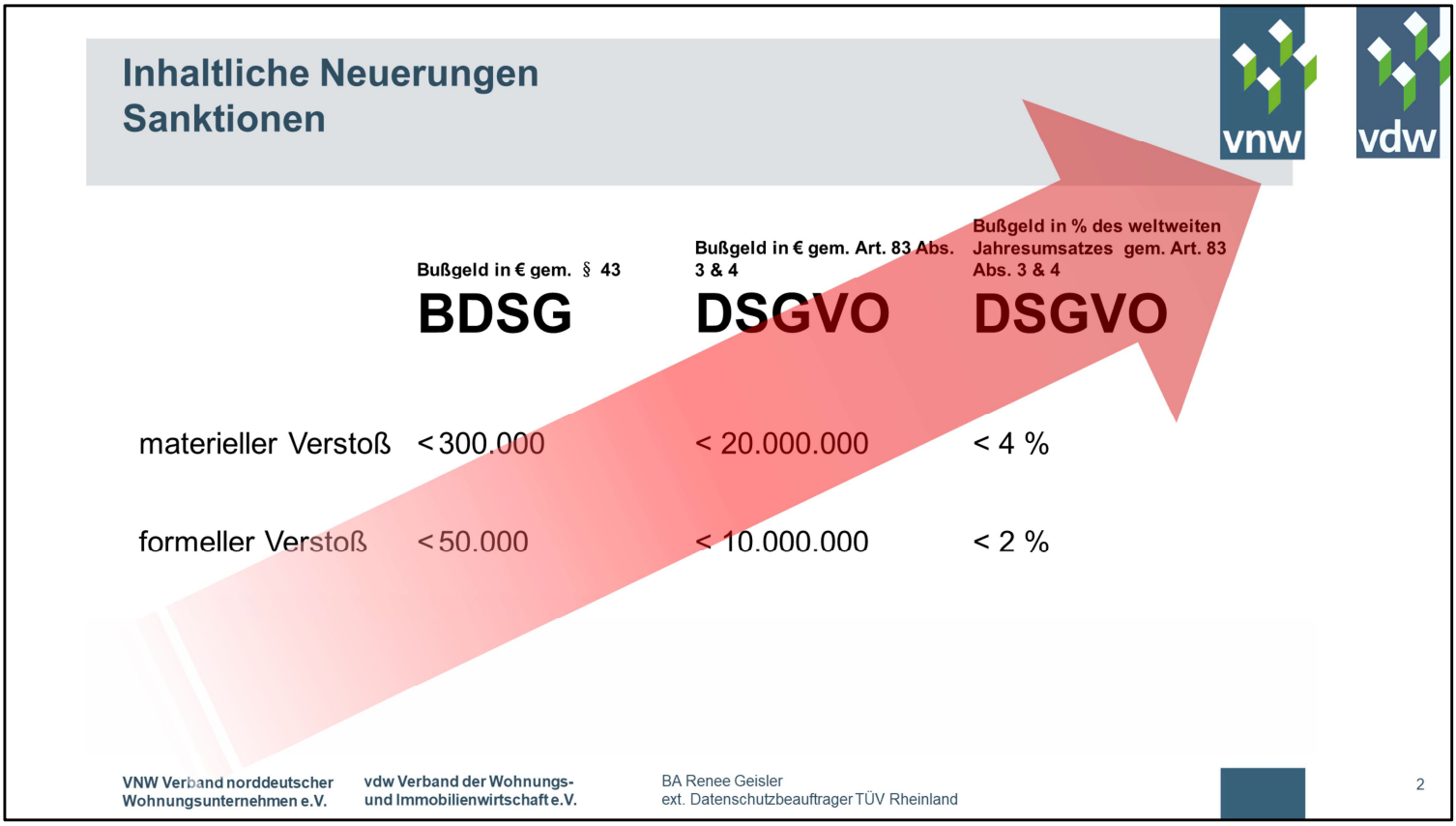
Datenschutzkonzept für Wohnungsunternehmen

Boltenhagen, den 25.06.2018

Bild: Tourismuszentrum Mecklenburgische Ostseeküste GmbH

VNW Verband norddeutscher Wohnungsunternehmen e.V.

vdw Verband der Wohnungs- und Immobilienwirtschaft e.V.



Individuelle Risikosituation des Unternehmens prüfen

Was geht nach Außen? Klassiker

. Mietinteressentenbogen – Nationalität. Diese pauschale Abfrage der Staatsangehörigkeit ist nie zulässig. Vgl. Orientierungshilfe DSK 30.01.2018

. Website – Datenschutzerklärung, wie Herr Maaß bereits ausführte

… und erfahrungsgemäß wird es dann sehr dünn von der Dokumentation

Inhaltliche Neuerungen
Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO

Verantwortlich für all das ist nicht der Datenschutzbeauftragte sondern der Verantwortliche (Art. 5 Abs. 2 DSGVO)

Sofern DSB auch handelnde Person ist genauso Auftragsdatenverarbeiter (Geschäftsbesorger) für handeln verantwortlich.

Der Datenschutz kommt an vielen verschiedenen Stellen im Unternehmen zum Einsatz und soll so von jedem Mitarbeiter gelebt werden (first line)

Die Datenschutzfunktion unterrichtet berät und überwacht die Einhaltung DSGVO und andere Datenschutzvorschriften (second line)

WhatsApp arbeitet mit Partnern, Dienstleistern und verbundenen Unternehmen zusammen, die uns dabei unterstützen, dir Möglichkeiten bereitzustellen, dich mit ihren Diensten zu verbinden. Wir verwenden die von ihnen erhaltenen Informationen, um unsere Dienste zu betreiben, bereitzustellen und zu verbessern.

Verbundene Unternehmen

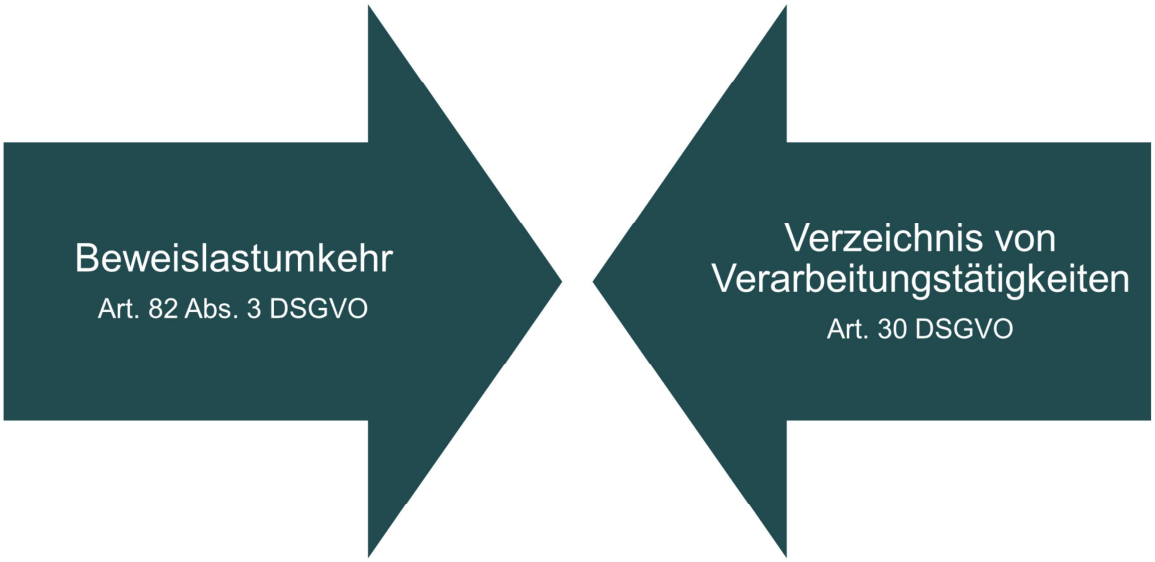
Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy)
Atlas (http://atlassolutions.com/privacy-policy)
Instagram LLC (http://instagram.com/about/legal/privacy/)
Onavo (http://www.onavo.com/privacy_policy)
Moves (http://moves-app.com/privacy)
Oculus (http://www.oculus.com/privacy/)
WhatsApp Inc. (http://www.whatsapp.com/legal/#Privacy)
Masquerade (https://www.facebook.com/msqrd/privacy)
CrowdTangle (https://www.crowdtangle.com/privacy)

Beispiel Crowd Tangle - Reichweiten Analyse Nachrichten

“Wir teilen Informationen weltweit im Einklang mit dieser Richtlinie, sowohl intern

zwischen den Facebook-Unternehmen (https://www.facebook.com/help/111814505650678) als auch extern mit unseren Partnern sowie mit denen, mit denen du dich auf der ganzen Welt verbindest und mit denen du etwas teilst.“

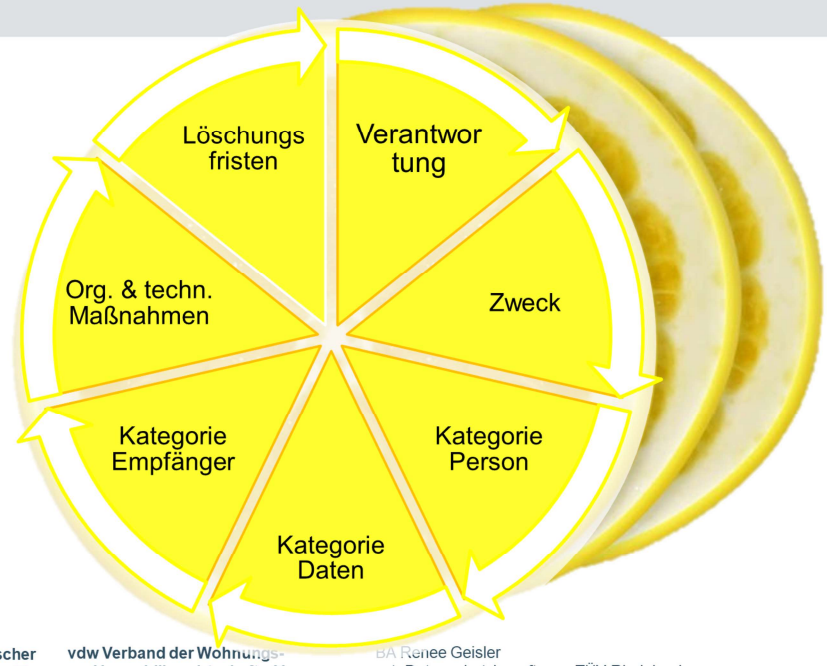
Inhaltliche Neuerungen
Dokumentation und Verfahrensverzeichnis I



Beweislastumkehr:

Der Verantwortliche kann nur von der Haftung befreit werden, wenn er nachweisen kann, dass er für die Umstände durch ein Schaden eingetreten ist nicht verantwortlich ist.

Inhaltliche Neuerungen
Dokumentation und Verfahrensverzeichnis II



Fehlt das Verzeichnis –> form. Verstoß –> bis zu 10.000.000 €

Allgemeine Beschreibung Organisatorische und technische Maßnahmen gem. Art. 32 Abs. 1 DSGVO

Doch das allein reicht nicht aus!

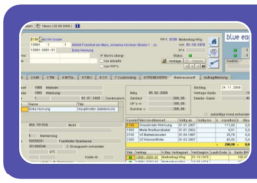
Diese Allgemeine Beschreibung einer Verarbeitung stellt noch keine ausreichende Dokumentation von Verarbeitugnstätigkeiten dar und erfüllt allein noch nicht die Anforderungen an die Transparenz gem. Artikel 5 DS-GVO.

Alle relevanten Komponenten müssen prüffähig sein

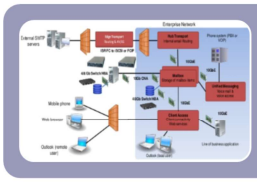
Die Funktionen aller Komponenten sollten für eine SOLL-IST Bilanzierung zugänglich sein

Inhaltliche Neuerungen
Ebenen des SDM

Zweckbestimmung
- Erforderlichkeit
- Gesetzl. Anforderungen



Fachapplikation
- Funktionalität
- Zweckbindung



IT - Infrastruktur
- Datenminimierung
- Transparenz

VNW Verband norddeutscher Wohnungsunternehmen e.V. | vdw Verband der Wohnungs- und Immobilienwirtschaft e.V. | BA Renee Geisler, ext. Datenschutzbeauftrager TÜV Rheinland | 7

Ebene 1
Bestimmung des Zwecks
- „Fachverfahren“ oder „Geschäftsprozess“ selbst
- Identifizierung von pbD und gesetzliche Anforderungen
- Festlegung der Rollen und Berechtigungen sowie der zur Verarbeitung zugelassenen Systeme

Ebene 2
Fachapplikation
- praktische Umsetzung durch die Sachbearbeitung
- Vollständige Erfüllung der funktionalen und rechtlichen Anforderungen obligatorisch
- Die Verarbeitung zusätzlicher Daten oder die zusätzliche Verarbeitungsformen sind auszuschließen
- KEINE Dehnung des Zweckes oder unterlaufen des Verarbeitungszweckes

Ebene 3
- Ansiedlung der technischen Services (Betriebssysteme, virtuelle systeme, Datenbanken, Authorisierungssysteme, Router, Firewalls, Speichersysteme wie z. B. NAS, Kommunikationsinfrastruktur,
- Damit hier der Zweck nicht gedehnt wird - Arbeitsanweisung/Betriebsvereinbarung
- ZIELE

- Datenminimierung, Nichtverkettung, Intervenierbarkeit

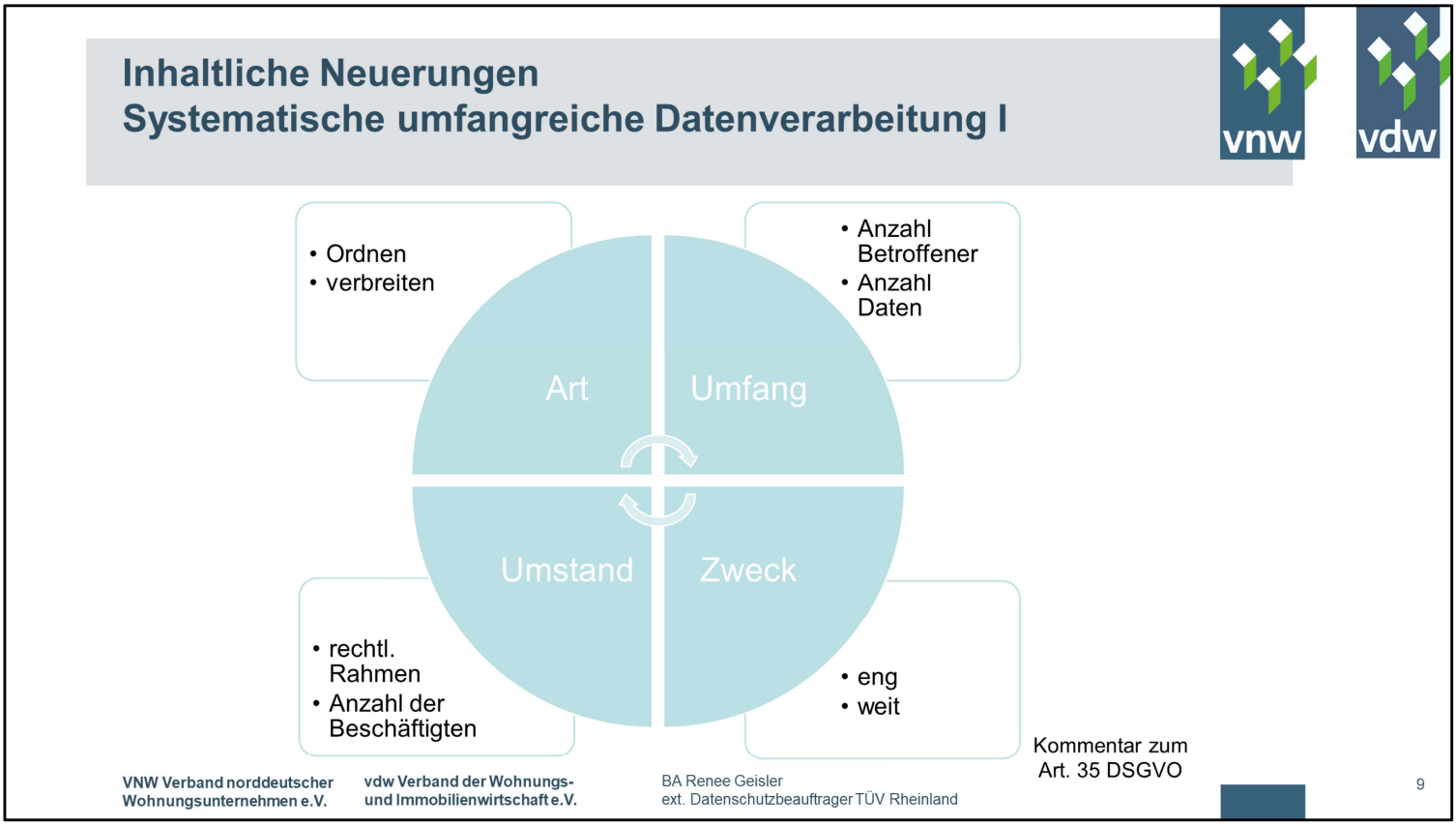
Inhaltliche Neuerungen
Anwendung eines SDM

Gewährleistungsziele

- Verpflichtungsgrad
- Qual. & quant. Parameter
- Schutzbedarf

Vergleich

- Inst. Kontext
- Techn. Org. Maßnahmen
- Wirksamtkeit
- Defizite?



<u>Formen der Verarbeitung:</u>

Neue Technologien – Videoüberwachung = systematisch und umfangreich zugleich!

Art – Ordnen oder verbreiten?

Umfang – Anzahl der Betroffenen / Anzahl ihrer Daten

Umstand – rechtliche Rahmenbedingungen Anzahl verarbeitender Personen

Zweck – Enge oder weite Zweckbindung

Auch One-Man-Shows gem. Artikel 37 müssen DSB bestellen da Datenverarbeitung:

- Die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche und systematische** Überwachung von betroffenen Personen erforderlich machen.

- Definition „umfangreich“ und „systematisch“ bei Datenverabeitung.

- **Umfangreich** ist die Datenverarbeitung i.S.d. Erwägungsgrundes (91) der DSGVO, wenn **große Mengen an Daten** auf regionaler, nationaler oder supranationaler Ebene verarbeitet werden, eine **große Zahl von Personen betreffen könnten** und wahrscheinlich ein **hohes Risiko für die Rechte und Interessen der Betroffenen** mit

sich bringen. Betroffen sind z.B. große Personalabteilungen, Banken…

Inhaltliche Neuerungen
Systematische umfangreiche Datenverarbeitung II

DSFA erforderlich	Kein Erfordernis
systematisch	gelegentlich
umfangreich	Im Einzelfall
umfassend	punktuell

Risikolage = Eintrittswahrscheinlichkeit x Schadensschwere

Hoher Schaden	Diskriminierung Rufschädigung
	Identitätsdiebstahl Verlust vertraulicher Daten
	Finanzieller Verlust Wirtsch. oder gesellschaftl. Nachteile

Besondere Kategorien

Im Wohnungsunternehmen gern genommen:

rassische und ethnische Her·kunft

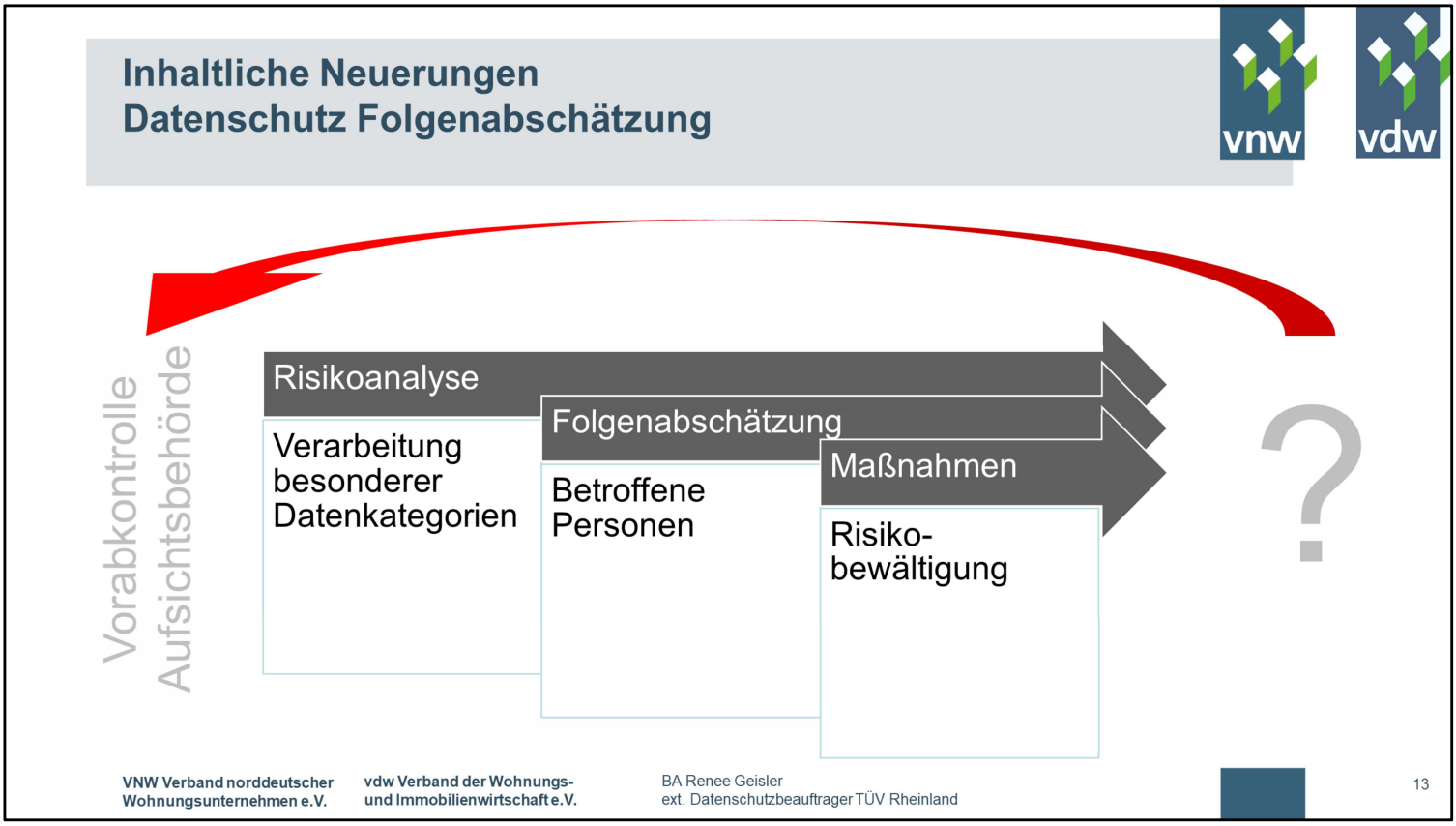
Substantiv [*die*]

1. Ort, Familie und Umgebung, in der man aufgewachsen ist.
   "Sie kann ihre einfache Herkunft nicht verleugnen."
2. Ort, an dem etwas hergestellt worden oder entstanden ist.
   "die Herkunft eines Produkts/einer Ware"

biometrischen Daten

Zusätzlich Allgemein:
politische Meinungen
religiöse oder weltanschauliche Überzeugungen
Gewerkschaftszugehörigkeit hervorgehen
genetischen Daten (
oder Daten zum Sexualleben
sexuellen Orientierung

Verarbeitung erlaubt in Deutschland nach §§ 22, 24 BDSG neu
Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit
Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich



Datenschutz Folgenabschätzung erforderlich bei…

- … der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO oder … Daten über strafrechtliche Verurteilungen und Straftaten Art. 10 DSGVO.

Jedoch kein abschließender Katalog. Entscheidend ist die Risikoanalyse

Veröffentlichungen der Aufsichtsbehörde : Hohes Risiko bei Profiling und Videoüberwachung.

Keine Datenschutz Folgenabschätzung bei: Keine Liste veröffentlicht (Stand nach der Recherche 29.08.2017)

Erforderliche Verknüpfung mit Verarbeitungsverzeichnis

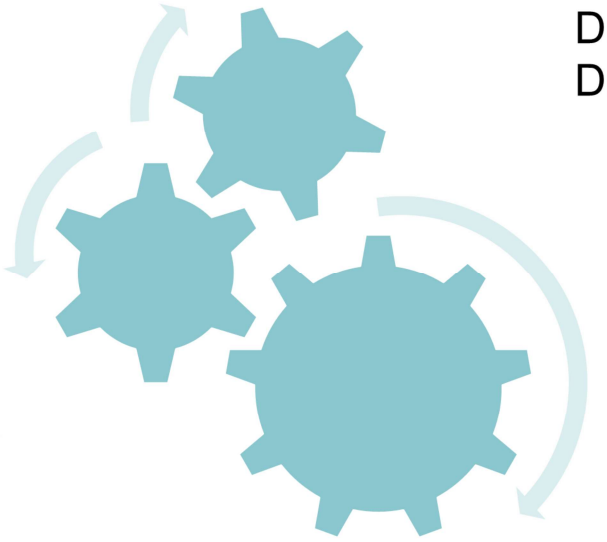
Beispiele
Privacy by Design & Standard

Grundsatz

Datenvermeidung und Datensparsamkeit

Privacy by Design

Datenminimierung



Privacy by Default

Erfordernis Verarbeitungszweck

VNW Verband norddeutscher Wohnungsunternehmen e.V. | vdw Verband der Wohnungs- und Immobilienwirtschaft e.V. | BA Renee Geisler, ext. Datenschutzbeauftrager TÜV Rheinland | 14

Frage ins Plenum:

Welche technischen und organisatorischen Maßnahmen gäbe es denn?

Individuelle Passwörter - alle 90 Tag ein neues komplexes Passwort (Groß und Klein und Sonderzeichen)

Übrigens:

Bereits begonnene Datenverarbeitungen, die auch schon vor dem 25.05.2016 begonnen haben bedürfen nur keiner erneuten Datenschutzeinwilligung, wenn der Art nach bereits der konform mit der DSGVO ist.

Ist sie es nicht sollte sie DSGVO-konform bis zum 25.05.2018 eingeholt werden.

Erwägungsgrund 171 Satz 3 DSGVO in Kombination mit Art. 6 (1) lt. b, c.

Folgen
Meldepflicht und Datenschutzverstöße

Verschärfung Notifikationspflichten

Jede Datenkategorie

72 Stunden Regelmeldefrist

Keine bestimmten Datenkategorien ausgenommen

Jeder Datenschutzverstoß geeignet eine Meldung an die Aufsichtsbehörde auszulösen, wenn damit ein Risiko für den Betroffenen einhergeht.

Bei hohem Risiko auch Meldung an den Betroffenen erforderlich.

Es ist zu Prüfen, ob das Unternehmen bereits über Prozesse zur Erkennung und Behandlung von Informationssicherheitsvorfällen/Datenschutzverstößen verfügt.

Bejahendenfalls sind diese anzupassen! Sonst Zuständgkeiten, Schnittstellen, Prozesse und Maßnahmen einführen und dokumentieren. Dabei Vorgaben zur Risikobewertung machen und Strukturen vorsehen die Meldung binnen 72 Stunden ermöglichen.

Vielen Dank für die Aufmerksamkeit