# Datentransfer und Informationspflicht: Herausforderungen für Rückversicherer

AIDA Swiss Chapter, GDPR/DSG Fokus Session, Konsequenzen für Schweizer Versicherer und Rückversicherer, 12. März 2018

Dr. iur. Nando Stauffer von May

Rechtsanwalt, Notar des Kantons Bern

gbf

recht@muri

gbf

1. Datenbearbeitung in der Rückversicherung
2. Fällt ein Schweizer Rückversicherer in den Anwendungsbereich der GDPR (DSGVO)?
3. Wie präsentiert sich die Situation eines Rückversicherers mit mehreren Niederlassungen weltweit?
4. Wie können Daten innerhalb der verschiedenen Niederlassungen rechtskonform transferiert werden?
5. Wie stellt der Rückversicherer die Informationspflicht gegen über den Datensubjekten (insb. Versicherte unter der Erstversicherung) sicher?
6. Wie lange darf der Versicherer die Daten aufbewahren?

# Rückversicherung

***Reinsurers*** provide insurance cover to another **insurer** or **reinsurer**. That insurance is known a reinsurance.

Insurance Market Core Uses Information Notice published by Lloyd's Market Association

# Datenbearbeitung in der Rückversicherung

## gemäss Lloyd's Market Association

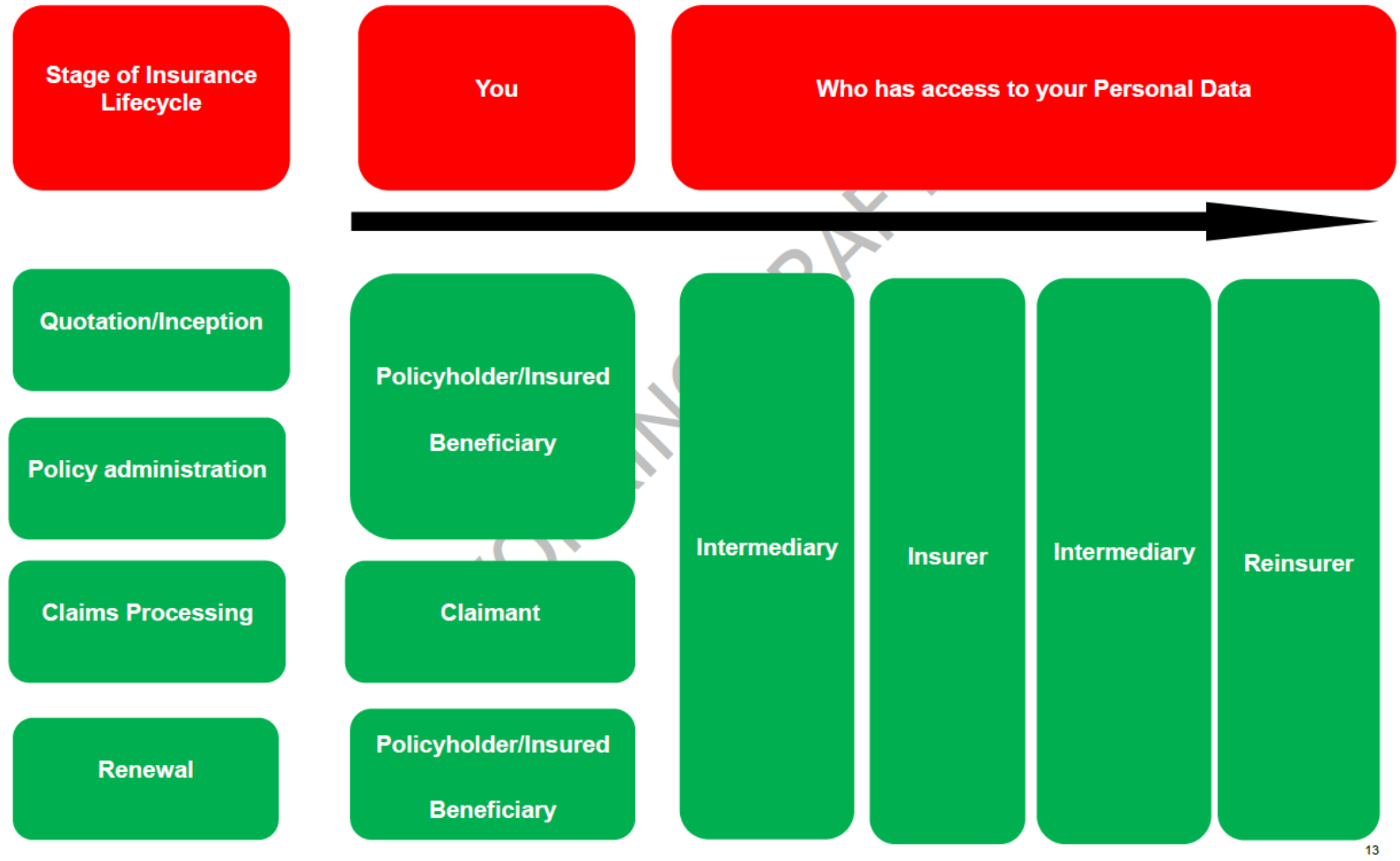
DATA PROTECTION

INSURANCE MARKET CORE USES INFORMATION NOTICE

Working draft 28 November 2017

# Datenbearbeitung in der Rückversicherung

APPENDIX 1: THE PURPOSES, CATEGORIES, LEGAL GROUNDS AND RECIPIENTS, OF OUR PROCESSING OF YOUR PERSONAL DATA



# Datenbearbeitung in der Rückversicherung

**Quotation / Inception**: Evaluating the risks to be covered & matching to appropriate policy/ premium

| | Categories of data | Legal grounds | |
|---|---|---|---|
| | **Personal data:**<br>• Individual details<br>• Policy information | **Personal data:**<br>• Legitimate interests (to determine the likely risk profile and appropriate insurance product and premium) | |
| | **Special categories of personal data:**<br>• Previous claims | **Special categories of personal data:**<br>• Consent | |

# Datenbearbeitung in der Rückversicherung

**Claims Processing**: Managing insurance claims including fraud, credit and anti-money laundering and sanctions checks.

| Categories of data | Legal grounds | Disclosures |
|---|---|---|
| **Personal data:**<br>• Individual details<br>• Policy information | **Personal data:**<br>• Legitimate interests (to assess the veracity and quantum of claims) | • Solicitors<br>• Experts<br>• [Loss adjustors?] |
| **Special categories of personal data:**<br>• Credit and anti-fraud data<br>• Risk Details<br>• Previous claims<br>• Current claims | **Special categories of personal data :**<br>• Consent<br>• Legal claims | |

| | | | |
|---|---|---|---|
| **THROUGHOUT THE INSURANCE LIFECYCLE**<br><br>**Transferring books of business, company sales and reorganisations** | **Personal data:**<br>• Individual details<br>• Policy information | **Personal data:**<br>• Legitimate interests (to structure our business appropriately)<br>• Legal obligation | • Courts<br>• Purchaser |
| | **Personal data and special categories of personal data:**<br>• Previous claims<br>• Current claims | **Personal data and special categories of personal data:**<br>• Consent<br>• [Substantial Public Interest] | |
| **THROUGHOUT THE INSURANCE LIFECYCLE**<br><br>**General risk modelling & underwriting** | **Personal data:**<br>• Individual details<br>• Policy information | **Personal data:**<br>• Legitimate interests (to build risk models that allow accepting of risk with appropriate premiums) | |
| | **Special categories of personal data:**<br>• Previous claims<br>• Current claims | **Special categories of personal data:**<br>Consent | |
| **THROUGHOUT THE INSURANCE LIFECYCLE**<br><br>**Complying with our legal or regulatory obligations** | **Personal data:**<br>• Individual details<br>• Policy information | **Personal data:**<br>• Legal obligation | • PRA, FCA, ICO and other regulators |

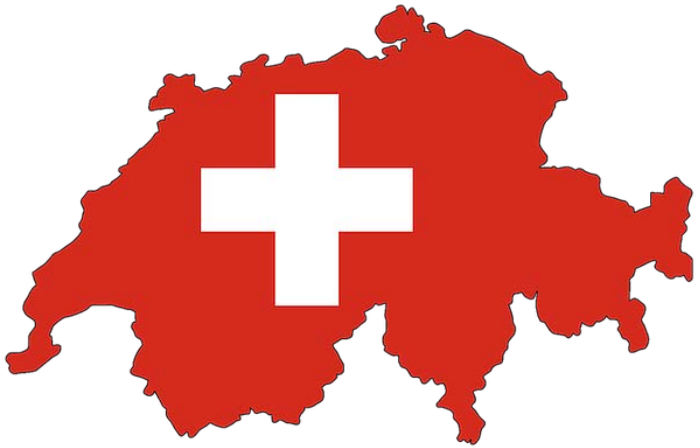
| Categories of data | Legal grounds | Disclosures |
|---|---|---|
| **Special categories of personal data:**<br>• Previous claims<br>• Current claims | **Special categories of personal data :**<br>• Consent<br>• Substantial Public Interest | |

# Weitere Datenbearbeitung

| Purpose | Categories of data | Legal grounds | Disclosures |
|---|---|---|---|
| **Recruiting and hiring employees and board members** | Resume, education documents of potential candidates irrespective of whether they are recruited or not; passport and other identification documents of employees and their family members, health related information, bank details etc. of employees. | Consent<br><br>Perform contract<br><br>Legal obligation | Tax and social security authorities, pension funds, insurance companies<br><br>Group Companies |
| **Payroll processing** | Bank details and details of salary of employees. | Consent<br><br>Perform contract | Bank, tax and social security authorities, pension funds<br><br>Group Companies |
| **Internal Audit** | As part of its role, a Group Internal Audit department audits various systems and processes and is likely to accesses Personal Data. | Perform a contract<br><br>Legal obligation<br><br>Legitimate interest (auditing) | Group Companies |
| **Service Agreement with third parties** | Service Agreements executed with third parties for various purposes is likely to contain Personal Data of signatories and people referred to in the Agreement. | Consent<br><br>Perform a contract<br><br>Legitimate Interest (doing business) | Counterparty |
| **Commercials** | Commercials may use Sensitive Personal Data of employees (pictures of employees). | Consent | Public |

# GDPR (EU-DSGVO) vs. DSG

gbf



# Räumlicher Anwendungsbereich

**Artikel 3 GDPR**

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese **im Rahmen der Tätigkeiten einer Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters **in der Union** erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. - > u.U. inkl. Werbe- oder Vertriebsniederlassungen (Representation Office)

(2) Diese Verordnung findet Anwendung auf die **Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen** Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) **betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) **das Verhalten betroffener Personen zu beobachten**, soweit ihr Verhalten in der Union erfolgt.

**(Marktortprinzip)**

**-> Rechtswahl ausgeschlossen**

# Räumlicher Anwendungsbereich

gbf

**Artikel 27 GDPR**

**Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern**

(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union.

(2) Die Pflicht gemäß Absatz 1 des vorliegenden Artikels gilt nicht für

a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder [...]

# Anwendungsbereich GDPR

(2) Diese Verordnung findet Anwendung auf die Verarbeitung **personenbezogener Daten von betroffenen Personen**, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) **betroffenen Personen** in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist

"It is not clear whether non-EU organisations offering goods and services do EU businesses (as opposed to individuals) will fall within the scope of "offering goods and services" test in Article 3(2)(a)."

Bird & Bird 2016

# Anwendungsbereich GDPR

Schweizer Rückversicherer (als Verantwortlicher) hat Auftragsverarbeiter in der EU (inkl. Cloud-Anbieter)

Schweizer Rückversicherer bearbeitet Daten (als Auftragsverarbeiter) für einen Verantwortlichen mit Niederlassung in der EU (z.B. Gruppengesellschaft)

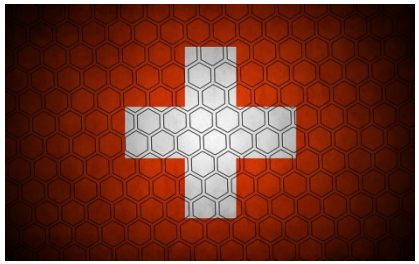
Alle mögliche Meinungen werden vertreten.
M.E. sollte GDPR für den Schweizer Rückversicherer nicht anwendbar sein.

Im Gegensatz zur *GDPR* (Art. 3) enthält der E-DSG keine besondere Bestimmung zum räumlichen Geltungsbereich des Gesetzes. Nach Auffassung des Bundesrates bietet bereits das geltende Recht die Möglichkeit, das DSG weitgehend auf Situationen mit internationalem Charakter anzuwenden. Aufgrund der Auswirkungstheorie gilt dies auch für das öffentliche Recht.

**oder**

Ausserdem ist zu berücksichtigen, dass schweizerische Unternehmen, welche in den Mitgliedstaaten der EU Dienstleistungen anbieten, die *GDPR* bereits aufgrund des darin vorgesehenen weiten räumlichen Anwendungsbereichs berücksichtigen müssen. Für diese Unternehmen führt der vorliegende Gesetzesentwurf nicht zu hohen zusätzlichen Kosten, da er ähnliche Massnahmen wie die europäische Verordnung enthält.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 (S. 79 und S. 250)



# Räumlicher Anwendungsbereich

**Art. 139 Abs. 3 IPRG (Privatrecht)**

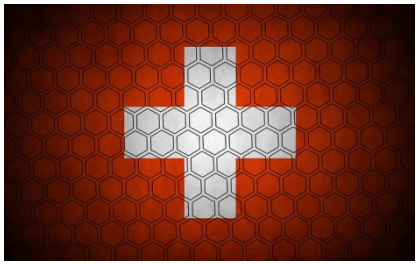
(1) Ansprüche aus Verletzung der Persönlichkeit durch Medien, […] unterstehen nach **Wahl des Geschädigten**:

a) dem Recht des Staates, in dem der Geschädigte seinen gewöhnlichen Aufenthalt hat, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste

b) dem Recht des Staates, in dem der Urheber der Verletzung seine Niederlassung oder seinen gewöhnlichen Aufenthalt hat, oder

c) dem Recht des Staates, in dem der Erfolg der verletzenden Handlung eintritt, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste.

(3) Absatz 1 ist auch anwendbar auf Ansprüche aus **Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten** sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten.



# Räumlicher Anwendungsbereich

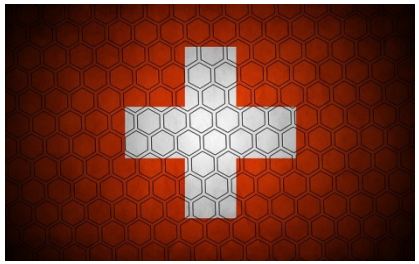
## Privatrecht

„Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden“ (Art. 15 Abs. 1 DSG).

DSG-widrige Bearbeitung von Personendaten = Persönlichkeitsverletzung

Sobald Daten die Schweiz verlassen, weiss der Verantwortliche nicht, welches Recht gewählt wird – er muss sich nach dem strengsten richten.

Keine vertragliche Rechtswahlmöglichkeit, da Haftung aus unerlaubter Handlung



# Räumlicher Anwendungsbereich

## Öffentliches Recht

Territorialitätsprinzip – Gebote und Verbote für Sachverhalte, die sich in der Schweiz zutragen = Verarbeitung in der Schweiz

*„Die in Street View verwendeten Bilder werden in der Schweiz aufgenommen, enthalten Informationen über Personen, Strassen und Plätze in der Schweiz und werden so veröffentlicht, dass sie in der Schweiz abrufbar sind. Es liegt somit ein überwiegender Anknüpfungspunkt zur Schweiz vor.“ (BGE 138 II 346 E. 3.3)*

Auswirkungsprinzip? Marktortprinzip?

**Strafrecht:** Erfolgsort oder Begehungsort in der Schweiz

961.011

# Verordnung über die Beaufsichtigung von privaten Versicherungsunternehmen

**(Aufsichtsverordnung, AVO)**

## 1. Titel: Geltungsbereich

**Art. 1** Versicherungstätigkeit in der Schweiz

[1] Eine Versicherungstätigkeit in der Schweiz liegt, unabhängig von der Art und vom Ort des Vertragsschlusses vor, wenn:

a. eine in der Schweiz domizilierte natürliche oder juristische Person zu den Versicherungsnehmern oder Versicherungsnehmerinnen oder zu den Versicherten gehört; oder

b. in der Schweiz gelegene Sachen versichert werden.

[2] Versicherungsunternehmen mit Sitz im Ausland ohne Niederlassung in der Schweiz unterstehen nicht der Versicherungsaufsicht, wenn sie in der Schweiz ausschliesslich folgende Versicherungsgeschäfte tätigen:

a. Deckung von Versicherungsrisiken im Zusammenhang mit Hochseeschifffahrt, Luftfahrt und grenzüberschreitenden Transporten;

b. Deckung für im Ausland gelegene Risiken;

c. Deckung von Kriegsrisiken.

[3] Die Absätze 1 und 2 gelten für die Versicherungsvermittlung sinngemäss.

recht@muri

# Weltweite Niederlassungen

# Weltweite Niederlassungen

Dear Sir/Madam,

Register your Data Protection Officer with us

From the findings of the PDPC's 2017 annual industry survey, we have identified a number of business sectors that ranked lowest[1] in terms of awareness and/or compliance with the Personal Data Protection Act (PDPA). Your company operates in one such sector. The PDPC is proactively reaching out to companies in these sectors to increase awareness and compliance with the PDPA, which is a law that applies to all organisations' collection, use and disclosure of personal data in Singapore.

Since 2016, nearly 40 organisations here have been found in breach of the PDPA were either issued warnings or directions. Some organisations have been directed to pay financial penalties[2]. A further 120 organisations were given advisory notices. Many of these cases could have been prevented if the organisation had appointed a Data Protection Officer (DPO) and taken adequate steps to comply with the PDPA in particular to protect the personal data they have collected.

An organisation that integrates personal data protection into its business processes and takes a proactive approach in fostering a data protection culture within the organisation will not only reduce the risk of data breaches, but can also reap the benefits of enhanced trust and goodwill with their customers. The PDPC has introduced a number of resources to help DPOs foster a data protection culture within their organisations, such as a DP Starter Kit and complimentary DP Advisory Services[3].

You should designate at least one individual as your DPO, which is mandatory under the PDPA, to help your organisation along this data protection journey. To better understand the role of a DPO, refer to www.pdpc.gov.sg/dpo.

# Weltweite Niederlassungen

Once you have appointed your DPO, you are strongly encouraged to register him or her with us at www.pdpc.gov.sg/dpo-contact so that your DPO can keep abreast of personal data protection developments and help your organisation comply with the PDPA.

We look forward to connecting with your organisation. Thank you.

Yours Sincerely,

Deputy Commissioner

---

[1] *Industries including Retail Trade, Finance and Insurance, Information and Communications, Accommodation, Food and Beverage, Healthcare, Employment and Professional, Scientific and Technical.*

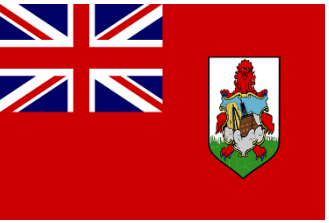
# Weltweite Niederlassungen

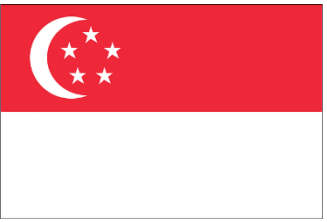
- **Special categories of personal data / besondere Kategorien personenbezogener Daten:** Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 GDPR)

- **Besonders schützenswerte Personendaten:** Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, die eine natürliche Person eindeutig identifizieren, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, **Daten über Massnahmen der sozialen Hilfe** (Art. 4 lit. c E-DSG)

CLASSIFIED

# Weltweite Niederlassungen





- "**Sensitive personal information**" means any personal information relating to an individual's **place of origin**, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, **marital status**, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information (Art. 7 para 1 Personal Information Protection Act 2016, Bermuda)
- **Keine gesetzliche Definition** in Singapur, aber für "sensitive personal data" gelten teilweise strengere Anforderungen (bspw. an Datensicherheit)
- Sensitive Personal Data: Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or **philosophical beliefs**, criminal record, trade-union membership and health or sex life (Data Protection Law 2007, applicable in the jurisdiction of the Dubai International Financial Centre).

DIFC

DATA PROTECTION LAW

DIFC LAW NO. 1 OF 2007

# Weltweite Niederlassungen

Missverständnisse mit lokalem Revisor, Finanzmarktaufsichtsbehörden, Datenschutzbehörden, Compliance- und Rechtsabteilungen sind vorprogrammiert.

# Weltweite Niederlassungen

Verarbeitung **bes. Kategorien personenbezogener Daten**

- Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt (Art. 9 Abs. 2 lit. a GDPR)
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des **Rechts eines Mitgliedstaats**, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, **aus Gründen eines erheblichen öffentlichen Interesses** erforderlich (Art. 9 Abs. 2 lit. g GDPR)

Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn Dritten **besonders schützenswerte Personendaten** bekanntgegeben werden (Art. 26 Abs. 2 lit. c E-DSG). Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, **durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist** (Art. 27 Abs. 1 E-DSG).

# Weltweite Niederlassungen

- Data Protection Bill

  Bill 153 2017-19, as brought from the Lords (18.01.2018), 2nd Reading House of Commons on 5 March 2018

  *"Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled…"*

- Schedule 1 – Special categories of personal data and criminal convictions etc data,
- Part 2 – Substantial public interest conditions

*Insurance*

15 (1) This condition is met if the processing –

(a) is necessary for an insurance purpose,

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

# Weltweite Niederlassungen

gbf



(c) is necessary for reasons of substantial public interest,

subject to sub-paragraphs (2) and (3).

(2) Sub-paragraph (3) applies where—

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

(b) the data subject does not have and is not expected to acquire—

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or

(ii) other rights or obligations in connection with such a contract.

(3) Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

# Weltweite Niederlassungen

gbf

## UK Data Protection Bill

(5) In this paragraph—

"insurance contract" means a contract of general insurance or long-term insurance;

"insurance purpose" means—

(a) advising on, arranging, underwriting or administering an insurance contract,

(b) administering a claim under an insurance contract, or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) Terms used in the definition of "insurance contract" in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.

CLASSIFIED

# Weltweite Niederlassungen

gbf

- Weiterverarbeitung (speichern genügt) in anderen EU-Staaten?
- Nach Brexit?
- Verarbeitung in der Schweiz

# Datentransfer

# Datentransfer

Transfer (bekanntgeben, übermitteln) = **Verarbeitung** im Sinne von Art. 4 Ziff. 2 GDPR bzw. **Bearbeiten** im Sinne von Art. 4 lit. d E-DSG

Grundsatz EU: Verbot mit Erlaubnisvorbehalt

Grundsatz Schweiz: Erlaubt, aber Verbotsvorbehalt

GDPR muss Datenbearbeitung durch den Rückversicherer gestatten

# Datentransfer

## Lloyd's Market Association, GDPR Overview for Underwriters

- GDPR prohibits the processing of personal data unless there are legal grounds to do so. Below are potentially relevant legal grounds you can rely upon under GDPR in order to process personal data and special categories of data:

| **Personal data** | **Special categories of personal data** |
|---|---|
| • Consent (processing permitted if the data subject has consented to the processing) | • Explicit Consent of the data subject (significantly harder to obtain and requires an affirmative action - see ICO draft guidance) |
| • Performance of a contract with the data subject (processing necessary for the performance of a contract to which the data subject is a party; or for the taking of steps at the request of the data subject with a view to entering into a contract) | • Legal claims (processing necessary for establishment, exercise or defence of legal claims) |
| • Vital interests (processing necessary to protect the vital interests of the data subject or other individual) | • Vital interests (processing necessary to protect the vital interests of the data subject or other individual) |

# Datentransfer

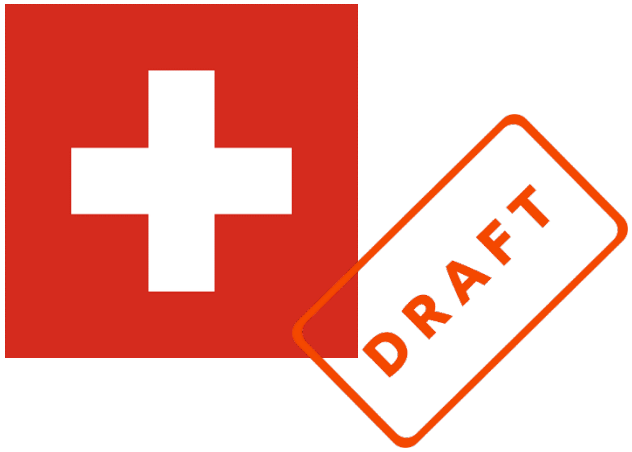
## Lloyd's Market Association, GDPR Overview for Underwriters

| | |
|---|---|
| • Legitimate interests (processing necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child) | |
| • In substantial public interest & set out in UK law | • In substantial public interest & set out in UK law<br>(processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject) |

# Datentransfer

**Outsoucring** an Auftragsverarbeiter gemäss Art. 28 GDPR grundsätzlich zulässig.

Verantwortliche, die Teil einer **Unternehmensgruppe** (...) sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem **Drittland** bleiben unberührt. (Erwägung 48 GDPR)




# Datentransfer

## 2. Abschnitt: Bekanntgabe von Personendaten ins Ausland

**Art. 13** Grundsätze

[1] Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

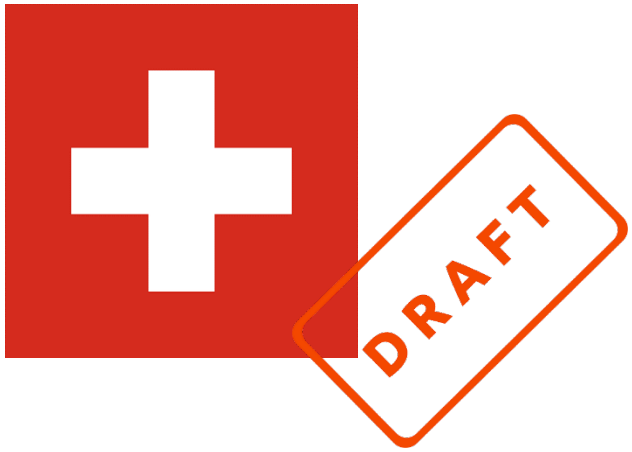
[2] Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

a. einen völkerrechtlicher Vertrag;

b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seinem Vertragspartner, die dem Beauftragten vorgängig mitgeteilt wurden;

c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem Beauftragten vorgängig mitgeteilt hat;

d. Standarddatenschutzklauseln, die der Beauftragte vorgängig genehmigt, ausgestellt oder anerkannt hat; oder




# Datentransfer

e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom Beauftragten oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

[3] Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.

**Art. 14** Ausnahmen

[1] Abweichend von Artikel 13 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden:

a. Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt.

b. Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags:
   1. zwischen dem Verantwortlichen und der betroffenen Person, oder
   2. zwischen dem Verantwortlichen und seinem Vertragspartner oder seiner Vertragspartnerin im Interesse der betroffenen Person.

c. Die Bekanntgabe ist notwendig für:
   1. die Wahrung eines überwiegenden öffentlichen Interesses, oder
   2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde.

# Datentransfer

**Kapitel 5:** Übermittlungen personenbezogener Daten an **Drittländer** oder an internationale Organisationen

**Art. 44 GDPR:** Allgemeine Grundsätze der Datenübermittlung

**Art. 45 GDPR:** Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

**Art. 46 GDPR:** Datenübermittlung vorbehaltlich geeigneter Garantien

Abs. 2 lit. b: **verbindlichen internen Datenschutzvorschriften** gemäß Artikel 47

Abs. 2 lit. c/d: **Standarddatenschutzklauseln** (von Kommission)

Abs. 3 lit. a: Vertragsklauseln (Genehmigung der Aufsichtsbehörde erforderlich)

**Art. 47 GDPR:** Binding Corporate Rules (BCR)

**Art. 48 und 49 GDPR:** Ausnahmen

# Datentransfer

**Weltweite Niederlassungen**:

- Intra Group Data Transfer Agreement
- Binding Corporate Rules

*„If an organisation is one legal entity, perhaps operating through a branch structure, then Model Clauses are not available. […] Once BCRs are in place, less time is required to be spent compared, for example, to maintaining Model Clauses.*“ (Allen & Overy LLP 2016)

# Datentransfer

## Intra Group Data Transfer Agreement

- Verwendung Standardklauseln
- Eigener Vertragstext genehmigen lassen
- In CH genügt evtl. Mitteilung (Art. 13 Abs. 2 lit. b E-DSG)
- Änderungen und Ergänzungen?

# Datentransfer

## Binding Corporate Rules (BCR)

Nicht nur bei rechtlichem Abhängigkeitsverhältnis im Konzern, sondern generell bei gemeinsamer wirtschaftlicher Tätigkeit möglich, nicht aber für externe Auftragsverarbeiter.

- Schutz auf Daten, die aus der EU stammen, begrenzen?
- Öffnungsklauseln für abweichendes DS-Recht
- Genehmigung durch EDÖB bzw. durch Lead Supervisory Authority

# Cross-border Processing

- Art. 4(23) GDPR: Verarbeitung erfolgt **in mehreren Mitgliedsstaaten** oder hat erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat

- **Lead Supervisory Authority** will be the Supervisory Authority of the main establishment or single establishment within the EU (Art. 56 GDPR)
- Main establishement = central administration within the EU, or place in the EU where the decisions about the means and purposes of the processing are made.

# Cross-border Processing

- If a company does not have an establishment in the EU then is must deal with Supervisory Authorities in every Member State they are active in, through local representative.
- There may be cases where a Controller has several establishments throughout the EU, but there is no EU Central Administration and none of the establishments take decisions about the processing activities in the EU (i.e. decisions are taken outside of the EU). In these cases the organisation is unlikely to be able to identify a Lead Supervisoriy Authority and will likely have to deal with various Supervisiory Authorities.

# Cross-border Processing

- Should an organisation wish to benefit from the one stop shop mechanism: designation of an establishment within the EU (as main establishment), which must have the authoritiy to implement decisions about the processsing activity and to take liability for the processing (including having sufficient assets)
- Fronting...

Gibraltar Regulatory Authority, Lead Supervisory Authority, Guidance Note IR02/17 of 24 May 2017

# Informationspflicht

# Informationspflicht

## Artikel 13 GDPR: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

## Artikel 14 GDPR: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) … f)

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) … g)

# Informationspflicht

**Artikel 14 GDPR**

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch **innerhalb eines Monats**,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die **Offenlegung an einen anderen Empfänger** beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten **für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden**, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

# Informationspflicht

**Artikel 14 GDPR**

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) **die betroffene Person bereits über die Informationen verfügt**,

b) die Erteilung dieser Informationen sich als **unmöglich** erweist **oder einen unverhältnismäßigen Aufwand erfordern würde**; [...]

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder,

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem **Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht**, unterliegen und daher vertraulich behandelt werden müssen.

# Informationspflicht

**Unmöglich oder unverhältnismäßige Aufwand:** In diesem Fällen ergreift der Verantwortliche geeignete **Massnahmen zum Schutz** der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschliesslich der Bereitstellung dieser Informationen für die Öffentlichkeit (Art. 14 Abs. 5 lit. b GDPR).

«Der voraussichtliche Aufwand der Mitteilung ist dem Informationsinteresse der betroffenen Person zuzuordnen. Dem Verantwortlichen ist ein umso höherer Aufwand zuzumuten, je wichtiger die Mitteilung ist, damit die betroffene Person von ihren Rechten wirksam Gebrauch machen kann, und je grösser die Risiken der Datenverarbeitung für die betroffene Person ausfallen.»
(Kühling/Buchner (Hrsg.), Datenschutzgrundverordnung, Beck 2017, Art. 14 N 55)

-> Interesse der betroffenen Person an Datenbearbeitung von Rückversicherern i.d.R. gering.

Schutzvorkehrungen: Veröffentlichung der Information, Dokumentationspflicht (weshalb betr. Informationen nicht mitgeteilt werden)

# Informationspflicht

**Artikel 18 E-DSG**

Abs. 2) Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht zudem, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die Information ist nicht möglich.

b. Die Information erfordert einen **unverhältnismässigen Aufwand**.

*«Der Aufwand für die Information der betroffenen Person ist unverhältnismässig, wenn der zu betreibende Aufwand im Verhältnis zum Informationszugewinn der betroffenen Person sachlich nicht gerechtfertigt erscheint. […] Diese Ausnahme ist eng auszulegen. Der Verantwortliche darf sich nicht mit der Vermutung begnügen, die Information sei unmöglich oder nur mit unverhältnismässigem Aufwand zu bewerkstelligen. Vielmehr hat er grundsätzlich sämtliche Vorkehren zu treffen, die unter den gegebenen Umständen von ihm erwartet werden können, um der Informationspflicht nachzukommen. Erst wenn diese erfolglos bleiben, darf der Verantwortliche davon ausgehen, die Information sei unmöglich.*» (Botschaft, S. 119)

# Informationspflicht

**Artikel 14 Abs. 5 lit. d GDPR**

die personenbezogenen Daten **gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten** dem **Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht**, unterliegen und daher vertraulich behandelt werden müssen.

**Art. 18 Abs. 1 lit. c E-DSG**

Es handelt sich beim Verantwortlichen um eine private Person, **die gesetzlich zur Geheimhaltung verpflichtet ist**.

Liechtensteinisches Landesgesetzblatt
Jahrgang 2015 Nr. 231 ausgegeben am 31. August 2015

# Gesetz
vom 12. Juni 2015
## betreffend die Aufsicht über Versicherungsunternehmen (Versicherungsaufsichtsgesetz; VersAG)

### Art. 104
*Geschäftsgeheimnis*

1) Die Mitglieder der Organe von Versicherungsunternehmen und ihre Mitarbeiter sowie sonst für solche Gesellschaften tätige Personen sind zur Geheimhaltung von nicht öffentlich bekannten Tatsachen verpflichtet, die ihnen aufgrund der Geschäftsverbindungen mit Kunden anvertraut oder zugänglich gemacht worden sind. Die Geheimhaltungspflicht gilt zeitlich unbegrenzt.

2) Vorbehalten bleiben internationale Abkommen, die gesetzlichen Vorschriften über die Zeugnis- oder Auskunftspflicht gegenüber den Gerichten, der Stabstelle FIU und den Aufsichtsorganen sowie die Bestimmungen über die Zusammenarbeit mit der Stabsstelle FIU oder mit anderen Aufsichtsbehörden.[5]

3. Versicherungsgeheimnis

Bisher konnte lediglich die Aufsichtbehörde das Versicherungsunternehmen gemäss Art. 44 Abs. 4 VersAG(alt) vom Versicherungsgeheimnis entbinden. Nach Inkrafttreten des revidierten VersAG können ausschliesslich die Versicherungsnehmer das Versicherungsunternehmen von der Geheimhaltungspflicht entbinden. Die FMA ist somit nicht mehr zuständig für die Entbindung. Eine globale Entbindung ist nach Art. 44 Abs. 4 VersAG nicht zulässig. Die Entbindungserklärung hat insbesondere folgende Voraussetzungen zu erfüllen:

- sie muss sich auf einen konkreten Einzelfall beziehen;
- sie muss in Kenntnis der Sachlage durch den Versicherungsnehmer erfolgen;
- sie muss in schriftlicher Form vorliegen.

Eine generelle Entbindung vom Versicherungsgeheimnis durch Aufnahme einer Bestimmung in den Allgemeinen Geschäftsbedingungen der Versicherungsunternehmen ist somit nicht zulässig.

Bezüglich den allgemeinen Anforderungen an Einwilligungen im Zusammenhang mit dem Datenschutzrecht kann auf die Ausführungen des Liechtensteinischen Datenschutzverantwortlichen verwiesen werden: http://www.llv.li/pdf-llv-li-die_einwilligung_als_zentrales_element_des_datenschutzrechts.pdf.

# Anwendbarkeit im EWR

Home - European Economic Area (EEA) / Relations with the EU

## European Economic Area (EEA) / Relations with the EU

The European Economic Area (EEA) unites the EU Member States and the three EEA EFTA States (Iceland, Liechtenstein, and Norway) into an Internal Market governed by the same basic rules. These rules aim to enable goods, services, capital, and persons to move freely about the EEA in an open and competitive environment, a concept referred to as the four freedoms. Read more...

GDPR ist nicht unmittelbar anwendbar

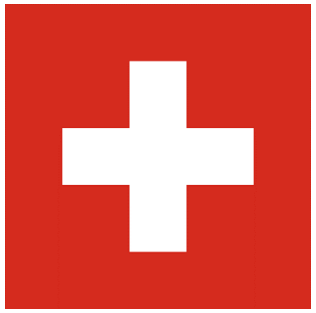
Diskussionen in Gemeinsamen EWR Ausschuss

Übernahme ist geplant

# Datenaufbewahrungsdauer

# Datenaufbewahrung

- **Information über die Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 13 Abs. 2 lit. a und Art. 14 Abs. 2 lit. a GDPR)
- Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“, Art. 5 Abs. 1 lit. c GDPR).
- Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit [...] („**Speicherbegrenzung**“, Art. 5 Abs. 1 lit. e GDPR).



# Datenaufbewahrung

- Art. 5 Abs. 4 E-DSG: Personendatenwerden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- Die Verpflichtung ergibt sich implizit auch aus dem allgemeinen Verhältnismässigkeitsgrundsatz, der in Absatz 2 der Bestimmung festgehalten ist. Der Bundesrat hält es indes für wichtig, diese Verpflichtung im Hinblick auf die technologische Entwicklung und die beinahe unbegrenzten Speichermöglichkeiten noch ausdrücklich festzuhalten. Die Einhaltung dieser Verpflichtung bedingt, dass der Verantwortliche **Aufbewahrungsfristen festlegt**. (Botschaft, S. 88)

# Datenaufbewahrungsdauer

## #6 of 9 – **Retention**

A data controller should ensure that personal information collected is not kept for longer than necessary in relation to the purpose(s) for which it was collected. Furthermore, an organisation should be clear about the length of time for which personal information will be kept and the reasons why it is being retained.

# Umfang der Datenbearbeitung

## #4 of 9 – **Adequate**

A data controller should ensure that personal information collected is adequate, relevant and not excessive in relation to the purpose(s) for which they were collected. Furthermore, a data controller should collect and retain only the minimum amount of personal information needed to achieve the established purpose(s).

In order to ensure that this requirement is met, please consider the following points in your self assessment:

- does the organisation collect all the personal information they need to serve their purpose effectively, and to deal with individuals in a fair and comprehensive manner?

- has the organisation checked to make sure that all the information collected is relevant, and not excessive, for purpose(s) specified?

- can the organisation justify every piece of personal information they hold on an individual if they where asked to do so?

# Datenaufbewahrungsdauer

## LMA Information Notice

### SECTION 8 RETENTION OF YOUR PERSONAL DATA

We will keep your personal data only for so long as is necessary and for the purpose for which it was originally collected. In particular, **for so long as there is any possibility that either you or we may wish to bring a legal claim under this insurance**, or where we are required to keep your personal data due to legal or regulatory reasons.

# Datenaufbewahrung

Erwägung 67 GDPR:

„Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentliche Daten vorübergehend von einer Website entfernt werden.“

Beschränkung statt Löschung im Sinne der Risikominimierung und Verhältnismässigkeit?

Dr. iur. **Nando Stauffer von May**

Rechtsanwalt, Notar des Kantons Bern