

VISCHER

The new Swiss Data Protection Act: Ten steps to consider for compliance

David Rosenthal
January 29, 2021

What happened so far

- On September 25, 2020, Swiss Parliament adopted a fully **revised Data Protection Act (DPA)**
 - Draft ordinances expected in Q1 2021
 - Entry into force **in 2022**, without transition period
- Switzerland **catches up with the EU** in data protection
 - Principle-based, not as detailed as the GDPR
- **But: No fundamental change** as to the basic concept
 - Previously permitted processing activities can generally continue
 - No copy of the EU General Data Protection Regulation (GDPR), but many regulations are adopted
 - Governance and data subjects' rights are expanded

Unofficial translation:
<https://bit.ly/3nKjiK1>
(datenrecht.ch)



<https://bit.ly/38MYISC>

Which processing is permitted?

No changes
needed

GDPR

- Basic processing principles must be complied with
 - Transparency, purpose limitation, fairness, data minimization, storage limitation, correctness, data security
- A legal ground is necessary
 - Contract, legal obligation, consent, legitimate interest, etc.

Revised DPA

- Same basic processing principles
- No legal ground required by default
 - A legal ground is only required if principles are *not* complied with, if sensitive data is disclosed to a third party or if the data subject objects
- The DPA is less strict on legal grounds for sensitive personal data

Rules for obtaining consent?

No changes
needed

GDPR

- Consent must be freely given, specific, informed and unambiguous
- No pre-ticked boxes
- May not be included in a contract unless necessary for its performance
- Data subject has to be informed of his/her right to withdraw consent
- Withdrawal at any time, fall-back on legitimate interest may be difficult

Revised DPA

- Must be freely given and informed
- Boxes may be pre-ticked on forms that contain an "acceptance" button
- May be included in a contract if there is a factual connection
- No information on right to withdraw required
- Withdrawal may be restricted in certain situations (e.g., related to costs)

Scope of Applicability

Verify scope of applicability

GDPR

- Processing of data about identified or identifiable individuals
- Automated processing and manual processing only if data is stored in a file
- Household processing exception
- Applies outside EEA if individuals are
 - targeted within the EEA for products or services
 - tracked within the EEA

Revised DPA

- Same definition of personal data
 - Legal entities no longer covered
- Any automated or manual processing of personal data (= broader scope)
- Exception for processing for personal purposes (private and business)
- Not applicable in legal proceedings
- Applicable if relevant activities, data subjects, the controller or processor are in Switzerland

Step 1: Update Privacy Policy

Privacy Policies should not only govern the collection of personal data on websites ...

- With the revDPA it will become mandatory
 - Information must be provided for each data acquisition
 - Posting on website, general terms and conditions/forms with link
- Minimum content defined, more only in exceptional cases
 - Identity, purpose of each procurement, categories of recipients, categories of data (if not obtained from the individual), countries, and justification for export to unsafe third countries
- Deliberate violation can be fined (CHF 250'000)
- **Practical tip:** Establish at an early stage within the company who collects which personal data and for which purpose (will help you develop the privacy policy as well as the inventory)
 - Processing activities required by law need not to be covered

Duty of Information

Privacy notice to
be amended

GDPR

- Whenever personal data is collected, a privacy notice has to be provided to the data subject
- Art. 13 et seq. defines the minimum content of the privacy statement
- Also applies if personal data is collected from a third party source
- Very limited exceptions

Revised DPA





- Similar information obligation whenever personal data is collected
- List of minimum information is shorter; information as per Art. 13 para. 2 GDPR necessary only under exceptional circumstances
- Broader exceptions (e.g., legal duty)
- **But:** Notice has to contain the list of countries to which personal data is transferred to and the legal grounds for transfers to unsafe countries

Soon to be released as
on a free license basis

Draft 7.06 – 12.01.21 – not yet released

DSAT.ch - Template Privacy Notice (general)

Privacy Notice of the [company] group

	
General Data We process general personal data about you.	Financial Data We process your financial data.
<i>[Note: concerns Section 3: all categories of data].</i>	<i>[Note: concerns Section 4: communication data, contract data].</i>
	

Will include "Privacy Icons"
courtesy of privacy-icons.ch

1.	What is this Privacy Notice about?	2
2.	Who is the controller for processing your data?.....	3
3.	What data do we process?	5
4.	For what purposes do we process your data?	10
5.	On what basis do we process your data?	14
6.	What applies in case of profiling and automated individual decisions?	15
7.	With whom do we share your data?	16
8.	Is your personal data disclosed abroad?	19
9.	How long do we process your data?	19
10.	How do we protect your data?	20
11.	What are your rights ?	20
12.	Do we use online tracking and online advertising techniques?	21
13.	What data do we process on our social network pages?	24
14.	Can we update this Privacy Notice ?	25

1. What is this Privacy Notice about?

The [company] group (also «we», «us») collects and processes personal data that concern you but also other individuals («third parties»). We use the word «data» here interchangeably with «personal data».

► More

In this Privacy Notice, we describe what we do with your data when you use [address of own website], our other websites or apps (collectively «website»), obtain services or products from us, interact with us in relation with a contract, communicate with us or otherwise deal with us. In addition, we may inform you about the processing of your data separately, for example in consent forms, terms and conditions, additional privacy notices, forms and other notices.

Draft 7.06 – 12.01.21 – not yet released

DSAT.ch - Template Privacy Notice (general)

with legal or contractual requirements, or for technical reasons. For contacts used only for marketing and advertising, the period is usually much shorter, usually no more than 10 years from the last contact.

More

Master data includes data such as name, address, e-mail address, telephone number and other contact details, gender, date of birth, nationality, data about related persons, websites, social media profiles, photos and videos, copies of ID cards; moreover, details of your relationship with us (customer, supplier, visitor, service recipient, etc.), details of your status, allocations, classifications and mailing lists, details of our interactions with you (if applicable, a history thereof with corresponding entries), reports (for example from the media), or official documents (for example excerpts from the commercial register, permits, etc.) that concern you. As **payment information**, we collect, for example, your bank details, account number and credit card data. Declarations of consent and opt-out information are also part of the master data, as well as information about third parties, for example contact persons, recipients of services, advertising recipients or representatives.

In relation with contact persons and representatives of our customers, suppliers and partners, master data includes, for example, name and address, information about the role or function in the company, qualifications and (where applicable) information about superiors, co-workers and subordinates and information about interactions with these persons.

Master data is not collected comprehensively for all contacts. The data collected in an individual case depends mostly on the purpose of the processing activity.

- **Contract data:** This means data that is collected in relation with the conclusion or performance of a contract, for example information about the contracts and the services provided or to be provided, as well as data from the period leading up to the conclusion of a contract, information required or used for performing a contract, and information about feedback (for example complaints, feedback about satisfaction, etc.). This includes health data and information about third parties, for example about hereditary diseases in a family. We generally collect this data from you, from contractual partners and from third parties involved in the performance of the contract, but also from third-party sources (for example credit information providers) and from public sources. We generally keep this data for 10 years from the last contract activity but at least from the end of the contract. This period may be longer where necessary for evidentiary purposes, to comply with legal or contractual requirements, or for technical reasons.

► More

- **Behavioral and preference data:** Depending on our relationship with you, we try to get to know you better and to tailor our products, services and offers to you. For this purpose, we collect and process data about your behavior and preferences. We do so by evaluating information about your behavior in our domain, and we may also supplement this information with third-party information, including from public

DSAT.ch - Template Privacy Notice (general)

NOT YET RELEASED

DSAT.ch - Template Privacy Notice (general)

Step 2: Create an Inventory

- All data processing activities have to be recorded
 - How you structure the directory is up to you
 - Not too many details needed, no personal data
 - Excel/Word instead of expensive software solutions are often ok
- DPA defines minimum content
 - Identity, purpose of processing, categories of recipients, categories of data, retention period, countries and how exports to unsafe third countries are secured
 - Shorter list for processors
- **Practical tip:** Combine this with Step 1, identify an owner for each processing activity and ask him/her to keep track of it
 - There are no fines

Documentation Duties

**Almost no
changes needed**

GDPR

- Records of processing activities
 - For controllers and processors
 - Defined content
- Principle of accountability
- Data Protection Impact Assessment
 - For likely high risk activities
 - Obligation to consult data protection authority if high risk remains despite all measures

Revised DPA

- Same records of processing activities
 - List all countries and legal grounds
- Comparable obligation to perform a Data Protection Impact Assessment
 - Legal ground needs not to be covered
 - Internal DPOs as an alternative solution for consultation of the data protection authority
- No principle of accountability

Step 3: Govern Processors

- If you delegate the processing of personal data to a service provider you must conclude a contract
 - Right to issue instructions, oversight, obligation to assist
 - Ensure data security
 - Use of sub-processors only with the controller's approval (new)
- But: A processor becomes a controller whenever using personal data for own purposes or determining key processing aspects
 - Even in such situations, a contract should be made
- Deliberate violation can be fined (CHF 250'000)
- **Practical tip:** You will already have suitable contracts with most service providers; check them to be sure

Controllers and Processors

Contracts to be amended

GDPR

- Art. 28 para. 3 GDPR specifies minimum content of data processing agreements
- Sub-processors require controller approval
- Art. 26 GDPR requires joint-controllers to define their respective responsibilities in an agreement
- Limited liability of processors

Revised DPA

- It adopts the concept of controllers and processors
- It does prescribe the content of a data processing agreement in the same level of detail, but it is to be drafted along same lines
 - Include references to the DPA and cover data exports correctly
- No express joint-controller duties
- Anyone participating in the violation of personality can be held liable

Step 4: Data Transfers Abroad

Revised EU SCC
expected soon

- Data transfers to "unsafe" third countries are only permitted with special precautions or in exceptional cases
 - The Federal Council will determine which countries are "safe"
 - Swiss regulation largely corresponds to the GDPR
- For exports to unsafe countries, the European Commission's "Standard Contractual Clauses" (SCC) are usually used
 - Due to "Schrems II", exports may require additional measures
- SCC alternatives: BCRs, contract performance, legal action
- Deliberate violation can be fined (CHF 250'000)
- **Practical tip:** Do you understand your data flows? Govern data flows contractually, even within your own group of companies

Data Export Rules

Separate, but
similar process

GDPR

- Transfers to countries without an adequate level of data protection not allowed without safeguards or based on an exemption
- Adequacy determined by EC
- Standard contractual clauses (SCC) and Binding Corporate Rules (BCR) may serve as safeguards
- Exemptions are available *inter alia* for the performance of a contract, for legal proceedings or with consent

Revised DPA

- Same concept
- Limitation only applies to transfers across the Swiss border
- Adequacy determined by Federal Council, will closely follow the EU
- EU SCC and BCR may, in principle, be used also for Switzerland
- Similar exemptions

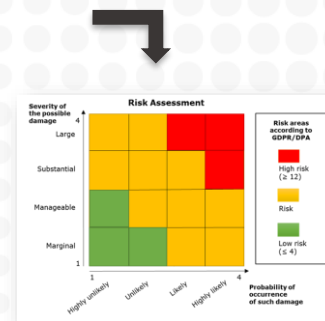
Step 5: DPIA

You can largely re-use
DPIAs created for the GDPR

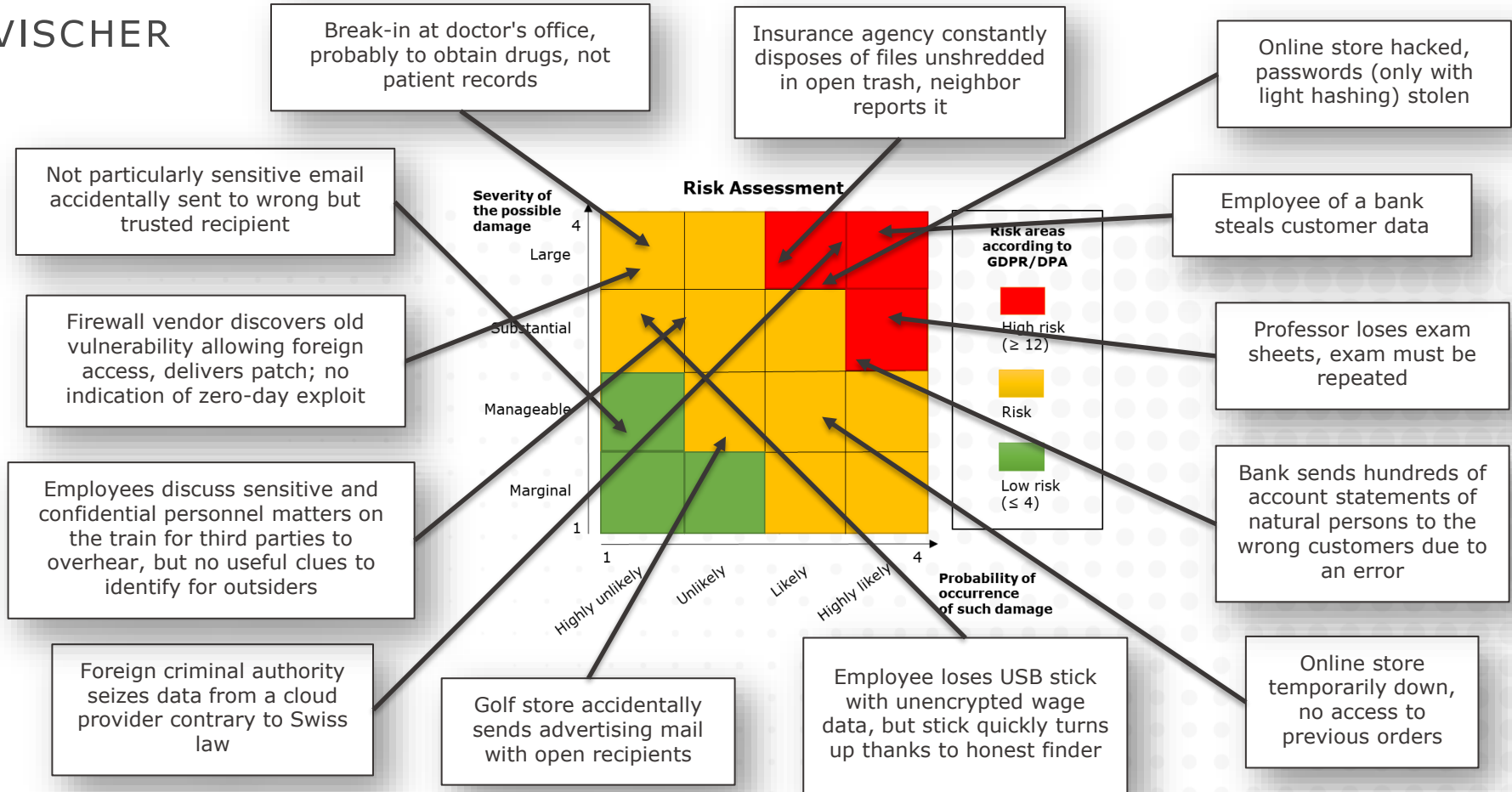
- If a data processing bears an increased risk to data subjects, a Data Protection Impact Assessment (DPIA) is necessary
 - Self-assessment exercise by the "business owner"
 - Description of the project, an analysis of possible (unintended) negative consequences for affected persons, countermeasures
- If a project involves a high risk despite all measures, the FDPIC (or data protection advisor) must be consulted
 - But: Violation is not sanctioned
- **Practical tip:** Create the DPIA together with the stakeholders from business, because only they know the project sufficiently well to provide the input needed and consider possible additional measures

Step 6: Data Breach Notifications

- Data breach: Unplanned breach of the confidentiality, integrity or availability of personal data (that takes corresponding effect)
 - Examples: Incorrectly sent mail, data loss, hacker accesses
- Notification to FDPIC only if there is a "high risk" of negative consequences for data subjects (concrete, not theoretical risk)
 - Notification as soon as the prescribed information is available
 - But: Violation is not sanctioned
- Must also be communicated to the data subject if necessary for his/her protection (e.g., to change password).
- **Practical tip:** Designate a responsible person and instruct employees to report incidents to him or her immediately
 - Processors must also report any and all data breaches



VISCHER



Data Breach Notifications

**Different
process needed**

GDPR

- Personal data breach = unplanned breach of confidentiality, integrity or availability of personal data
- Data breaches with a risk of negative consequences for data subjects need to be reported to the data protection authority within 72 hours
- Data subjects need to be informed if the breach poses a high risk
- Processors need to inform controller of any breach

Revised DPA

- Same definition of a "data breach"
- Same obligations for processors
- Reporting to the data protection authority only in cases of high risk
- No 72 hour deadline, no duty to keep records of data breaches
- A data subject need to be informed "if necessary for his/her protection"
- Exception in case of excessive costs

Step 7: Data Subject Rights

Access requests can often be answered in a standardized way
– prepare for this

- Data subjects can request access to their data (in some cases even in electronic form), ask for rectification and object
 - These rights are no absolute rights; they can be limited by the controller on certain grounds (e.g., certain overriding interests)
 - Data subject rights are usually free of charge
 - Proper identification of the requestor
 - The scope of the right to "data portability" remains unclear
- New more protection against abusive requests for information
 - Responding within 30 days, no need to confirm "completeness"
 - Deliberate violation can be fined (CHF 250'000)
- **Practical tip:** Designate a responsible person for such requests and check out the potential data sources already in advance

Right of Access

**Provide for
separate
guidelines**

GDPR

- Upon request, a controller shall provide the data subject
 - a copy of his/her personal data
 - certain ancillary information
- Data subject may ask for a copy
- Manifestly unfounded or excessive requests may be refused or a fee may be charged
- Exceptions available to protect third parties and business secrets

Revised DPA

- Same concept, but
 - the list of ancillary information that can be requested is shorter
 - additional information on countries to which data is transferred and legal grounds
 - data subject may ask for other useful information
- Fees? Yet to be clarified
- Protection of business secrets weak

Other Data Subject Rights

**No changes
needed**

GDPR

- Right of rectification
- Right to erasure/to be forgotten
- Right to restriction
- Right to object
- Right to data portability
- Obligation to notify third parties of such rights being exercised

Revised DPA

- The same data subjects rights also exist under the DPA
- The Swiss version of the "right to object" already includes the right to erasure and restriction; it can be overruled by an overriding private interest
- Very limited exceptions to the right to correct (legal obligation, archival purpose of public interest)
- No obligation to notify third parties

Step 8: Do you let computers decide?

- Automated Individual Decisions = discretionary decision with a legal or other similarly significant negative consequence, which is made entirely by a computer and concerns one individual
 - Example: Automatic job applicant selection or credit approval
 - Not in scope: Mere "if-then" decisions (no discretionary decision) or decisions prepared by a computer (not fully automated)
 - Such decisions are permitted in principle, but the data subject must be informed and, if desired, be heard by a human being
- No such protections where the data subject has consented to the decision being automated or where the decision matches the data subject's request (e.g., online store purchase)
- **Practical tip:** Automated individual decisions do not occur often, check within your company in advance

Automated Individual Decisions

No changes
needed

GDPR

- Right not to be subject to automated individual decisions or profiling that have legal or material negative effect
- Such decisions are allowed for concluding or performing contracts, where permitted by law or based on explicit consent, but come with
 - A right to human intervention
 - Information obligation

Revised DPA

- Automated individual decisions are defined in the same manner, but do not include profiling
- No prohibition or right of objection
- Similar right to human intervention and information obligation, except where the decision has been taken
 - as per the data subject's request (e.g., online-shop), or
 - with the data subject's consent

Step 9: Other Innovations

Most common problem is that data is kept longer than necessary

- Genetic and biometric data (for identification) are now also considered sensitive personal data
 - Legal consequence: The disclosure of such data to third parties requires some form of justification; consent must be explicit
- Data processing for non-personal purposes (e.g. research, statistics) is subject to slightly stricter rules than today
- Principle of "Privacy by Default": Make sure that default privacy settings in online services reflect the least invasive choice
- Profiling with and without "high risk" was discussed in detail in pariliamnt, but there are not many restrictions
- **Practical tip:** The new DPA is a good opportunity to check your processing activities for conformity using a risk based approach

Data Security, Privacy by Design

No changes
needed

GDPR

- Technical and organizational measures to ensure a level of data security appropriate to the risk
- Measures to ensure other aspects of compliance ("Privacy by Design")
- "Privacy by Default"
 - By default, personal data shall be limited to a minimum
 - No publication without approval by the data subject

Revised DPA

- Same level of data security required under the DPA
- Similar duty on "Privacy by Design"
- "Privacy by Default"
 - By default, end-user privacy settings (if any) must be set to the least invasive option offered
 - Override possible by way of advance agreement

Step 9: Other Innovations

Check whether an extension of your T&Cs and privacy statements makes sense

Art. 62 Breach of professional confidentiality

¹ If a person wilfully discloses secret personal data of which he has gained knowledge while exercising his profession which requires knowledge of such data, he shall be liable on complaint to a fine of up to 250,000 Swiss Francs.

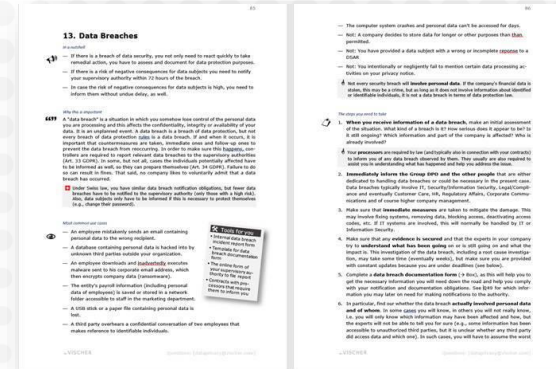
² The same penalty applies to anyone who wilfully discloses secret personal data of which he has gained knowledge in the course of his activities for a person bound by a confidentiality obligation or in the course of training with such a person.

³ The disclosure of secret personal data remains punishable after termination of such professional activities or training.

Step 10: Instructions, Training

If possible, build up data protection expertise internally

- Without appropriate instructions, your employees do not know what they must and may do
 - Adapt instructions and guidance in good time
 - Create templates, forms and checklists
 - Conduct training, log attendance
 - This is how you document compliance with the DPA, should you ever become the target of a proceeding
- But: A "data protection officer" is not mandatory
- Practical tip:** In view of the criminal sanctions under the revised DPA, it will become easier to motivate the business and management to act on data protection compliance



Sample data protection handbook

Data Protection Officer & Rep

No changes
needed

GDPR

- Data Protection Officer (DPO) required if processing involves
 - Regular/systematic monitoring or
 - Special categories of data (many)
- GDPR defines its DPOs independency, status, tasks and other prerequisites
- Foreign controllers and processors are to appoint a EU representative if certain thresholds are surpassed

Revised DPA

- No obligation to appoint a DPO
- Swiss law provides for a similar role, a.k.a. the "Data Protection Advisor"
 - Prerequisites are comparable
 - Permitted to judge DPIAs instead of the data protection authority
- Foreign controllers require a Swiss representative if they target or track Swiss data subjects and perform a high-volume, high-risk processing

Enforcement & Fines

**Personal
criminal liability**

GDPR

- Data protection authorities may
 - Investigate processing activities
 - Issue orders to restrict, change or stop processing activities
 - Issue fines of up to EUR 10/20m or 2/4% of the annual turnover for violation of most GDPR provisions
- Local law may provide for additional fines

Revised DPA

- Data protection authority may
 - Investigate processing activities
 - Issue orders to restrict, change or stop processing activities
- Cantonal authorities may
 - Issue fines against individuals of up to CHF 250'000 in case of intentional breach of certain DPA provisions or failure to cooperate with the data protection authority
 - No insurance/indemnification

Final Remarks

- Data protection compliance is a **Sisyphean task**
 - No one can fully comply with the DPA
- **Start the** implementation work already now
 - Dependency on other stakeholders within the company
 - In addition to their day-to-day business, they often have little desire to engage in data protection compliance
 - Many of the new "measures" are already expected today, whether from the FDPIC, under the GDPR or as part of good data protection compliance and governance
- The basic principles of data processing do not change, but are brought more into **focus**
 - The FDPIC will increase his activities, but fines will remain limited



Titian, 1548

VISCHER

Register for updates of our
Data & Privacy Blogs on
www.vischer.com

Thank you for your attention!

Questions: drosenthal@vischer.com

Zürich

Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel

Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf

Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00