

# VISCHER

## The new Swiss Data Protection Act: How does it compare to the GDPR?

David Rosenthal  
October 14, 2020

---

## We do it better in Switzerland!

- The new Swiss Data Protection Act (DPA) will most likely **come into force in 2022**
- Principle-based, not as detailed as the GDPR
- Governs both the processing by the private sector and Swiss Federal public authorities (here we will cover only the former)
- **Bottom line:** Compliance will not be too complicated to achieve if you already are GDPR-compliant
- I will speak about:
  - Conceptual differences with the GDPR to keep in mind
  - Situations where the DPA is less strict or stricter
  - Situations where the DPA is comparable

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

## 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 when 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

# Information Obligations

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

Fines!

## 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

Fines!

## 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



# 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

**Fines!**

## 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

# 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

Fines!

# 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

Fines!

# 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

## 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

## 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

# Professional Secrecy

**Personal  
criminal liability**

## GDPR

- n/a

## Revised DPA

- Obligation of a professional to keep confidential
  - secret personal data learned while exercising his or her profession
  - provided the profession requires knowledge of such personal data
- Only intentional acts
- Protects customers; waivers possible, but not always needed
- Personal fine of up to CHF 250'000

Fines!



## 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

**Fines!**

## Final words

- Data protection compliance will become **more burdensome** in Switzerland going forward
- Risk of personal criminal sanctions will cause individuals who are responsible for data protection compliance (and their advisors) to become **more cautious** than in the past
- Level of data protection will be similar as in the EEA, but expect to see a **more pragmatic approach** in Switzerland with regard to day-to-day compliance issues than in other countries
- The differences between the GDPR and the DPA will become relevant mainly for handling **individual cases** (e.g., disputes over the right of access)
- Nobody will ever be **fully compliant** – this will not change

# VISCHER

Register for updates of our  
**Data & Privacy Blogs** on  
[www.vischer.com](http://www.vischer.com)

## Thank you for your attention!

Questions: [drosenthal@vischer.com](mailto:drosenthal@vischer.com)

### Zürich

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

[www.vischer.com](http://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

If you wish to receive a copy of my detailed commentary on the new provisions, send me an e-mail (appears in November, in German).  
Summary: <https://bit.ly/36R5fMF>