New Swiss Data Protection Act

What IT professionals need to know and how they can contribute to operationalizing compliance

Thomas Steiner

LAUX LAWYERS AG
ZURICH | BASEL

Swiss Informatics Society

Evening Talk on nFDPA

October 20, 2022

Agenda

LAUX LAWYERS AG
ZURICH | BASEL

- New Swiss Federal Data Protection Act (nFDPA) – the Requirements at a Glance
- What to Do – seven Tasks
- Focus Topics for IT Professionals

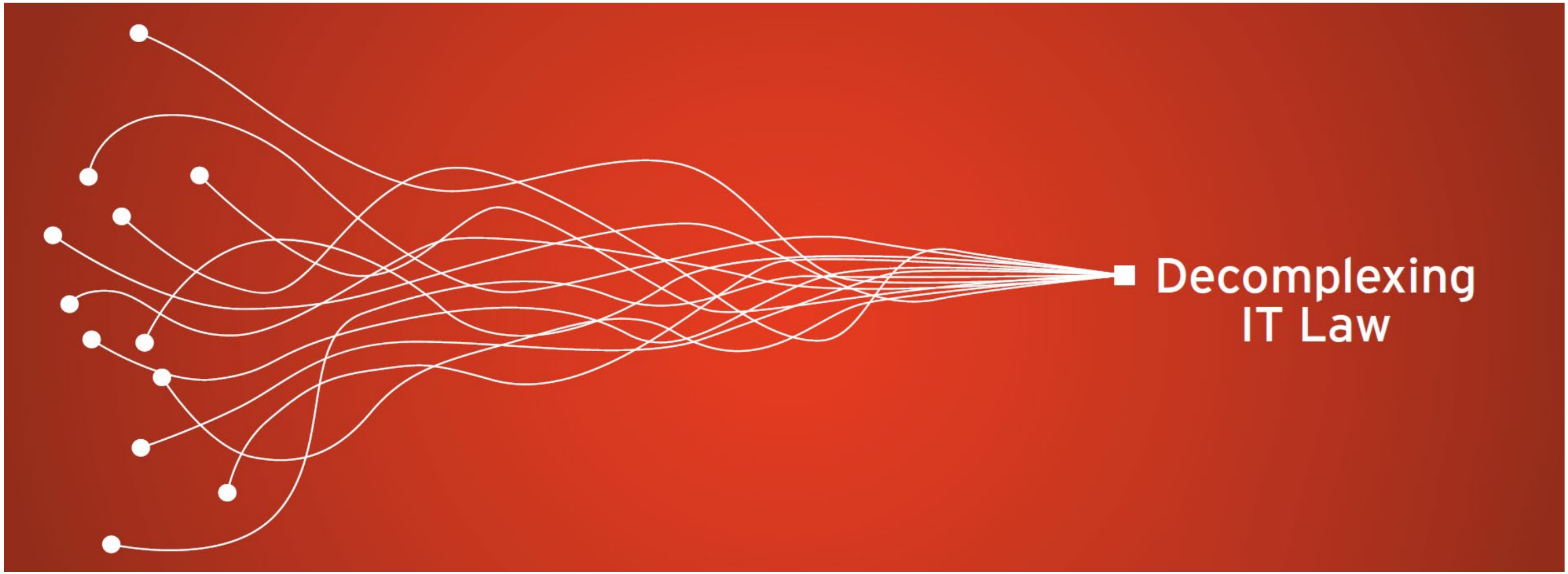
  (1) Data Security

  (2) Records of Processing Activities

  (3) Control over Service Providers (Outsourcing)
- Annex: nFDPA Implementation Check List

The nFDPA – Requirements at a Glance

LAUX LAWYERS AG
ZURICH | BASEL



nFDPA (in force from September 1, 2023)

LAUX LAWYERS AG
ZURICH | BASEL

Fed. Agencies: Legal Basis
(**Private organizations: basis for justification, where necessary!**)

Processing Principles
(Lawfulness, fairness / transparency, purpose limitation, data minimization / storage limitation, accuracy, security)

Transparency
(Duty to inform)

Data Subject Rights
(Rights of access and information, data portability, rectification, objection, deletion and deletion)

Documentation / Governance

Control over Service Providers
(Outsourcing)

International Data Transfers
(Across Swiss border)

Automated individual decision-making

Data Protection Impact Assessment / Privacy-by-Design and Default

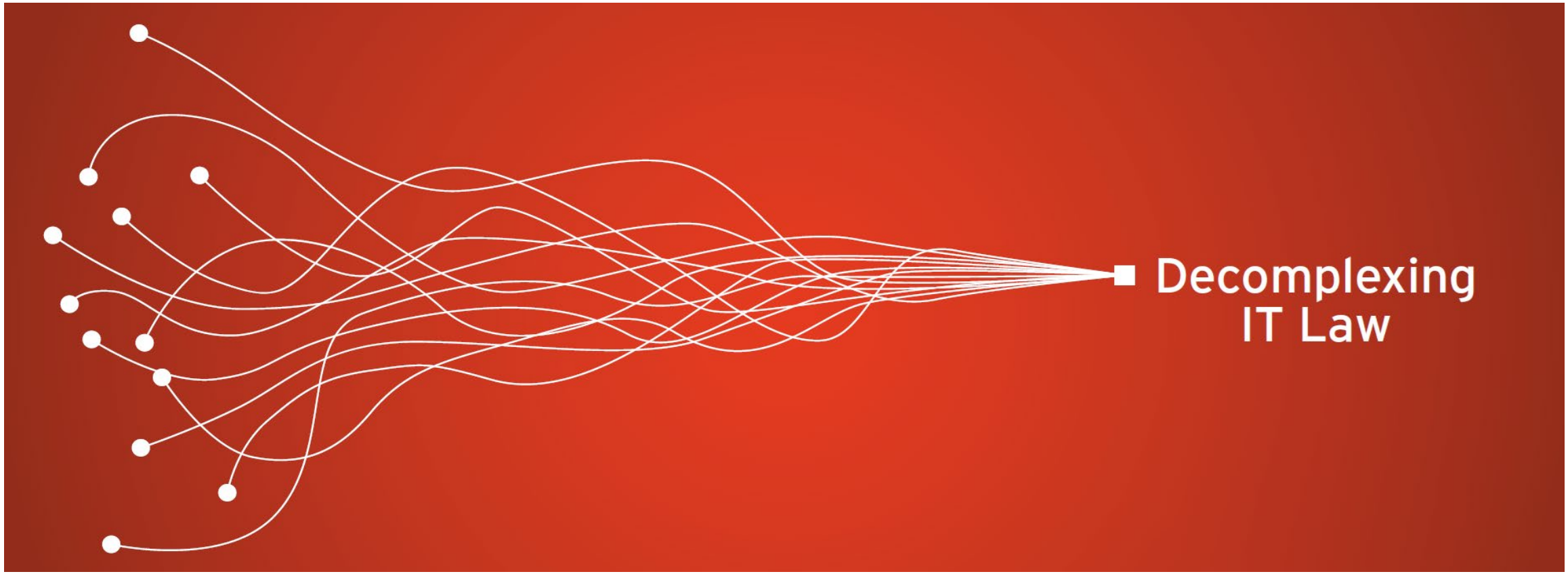
Data Breach Notification

Data Security

Enforcement

What to Do – seven Tasks

LAUX LAWYERS AG
ZURICH | BASEL



Seven Tasks

LAUX LAWYERS AG
ZURICH | BASEL

(1) Security! Without it "everything is nothing"

(2) Document your processing operations

(3) Provide for written agreements with your service providers

(4) Transparency! You need a general Privacy Notice (customer-facing)

(5) You need an Employee Privacy Notice (internal)

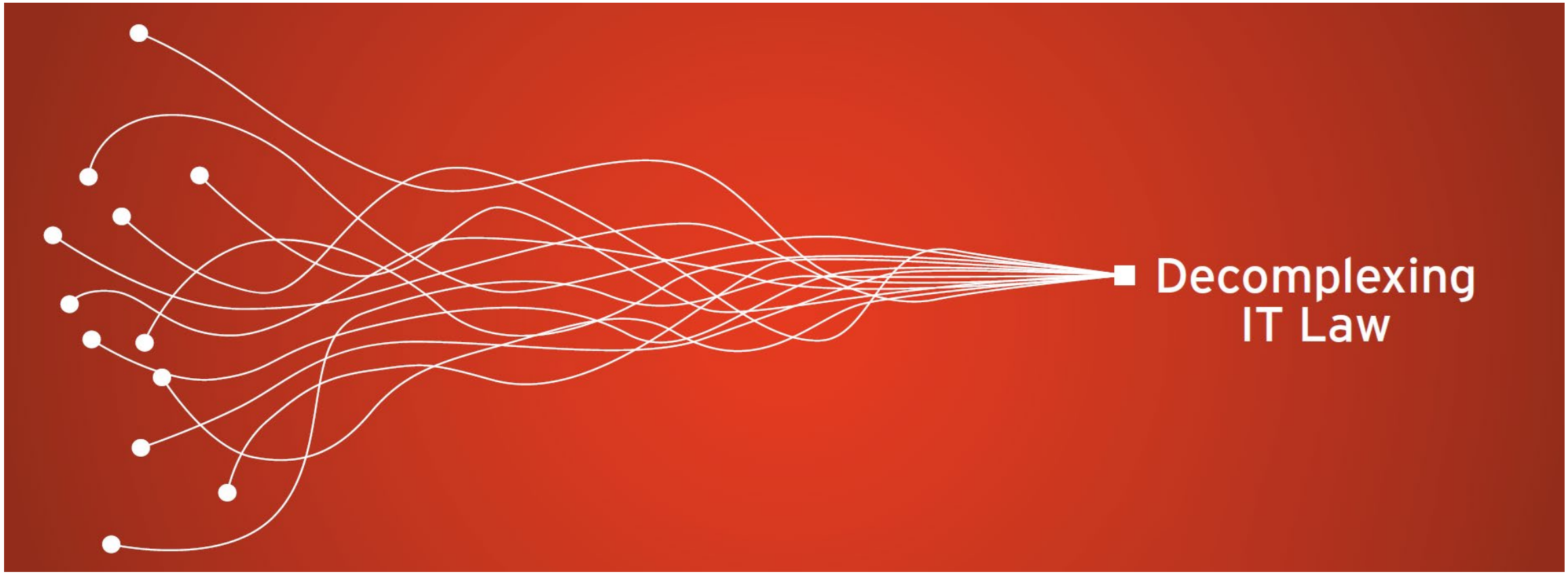
(6) Get organized to respond quickly to questions (internal guidelines)

(7) Document sufficient safeguards before disclosing data to recipients outside of Switzerland

(Focus topics for IT professionals in bold print)

Focus Topic #1: Data Security

LAUX LAWYERS AG
ZURICH | BASEL



Data Security (1|5)

Art. 8 nFDPA; Art. 2 of the new Data Protection Ordinance (nFDPO)

LAUX LAWYERS AG
ZURICH | BASEL

Art. 8 nFDPA – Data Security

*(1) The controller and the processor shall take appropriate technical and organizational measures to ensure data security **adequate** to the risk[s for individuals].*

(2) The measures must enable the avoidance of data breaches

*(3) The Federal Council shall issue provisions on the **minimum requirements** for data security.*

Art. 2 nFDPO – Objectives

- Confidentiality
- Integrity
- Availability
- Traceability

Data Security (2|5)

Arts 1 nFDPO

Determining Risks for Individuals considering

- cause of the risk
- main hazards
- measures planned to reduce the risk
- likelihood and severity of data breaches

Determining required level of protection, considering

- the *type* of personal data processed; and
- the *purpose, type, scope and context* of processing

Determining technical and organizational measures (TOMs), considering

- the state of the art; and
- the costs for implementation

Data Security (3|5)

Arts 3–4 nFDPO

TOMs (details of protection goals)

Confidentiality:

- Access control (physical and logical)
- User control (use by authorized persons only)

Integrity and Availability:

- Storage, media and transport control (prevent unauthorized reading, copying, alteration, shifting or deletion – at rest and in transit)
- Ability to restore (adequate back-ups)
- Reliability (and resilience) of systems

Traceability:

- Input control
- Disclosure control
- Detection and remediation of data breaches
- Keeping logs (Art. 4 nFDPO)

Data Security (4|5)

Art. 5 lit. h and Art. 24 nFDPA; Art. 15 nFDPO

- Data breach: *unintentional or unlawful loss, deletion, destruction or modification of personal data; or personal data being disclosed or made accessible to unauthorized persons*
- Notification by controller to FDPIC only in cases of "high risk"
- Notification by controller of (high-risk) data breach to data subjects (a) if necessary for the protection of the data subjects or (b) if the FDPIC so requests.
- No 72-hour deadline (“as soon as possible”; staggered notices allowed)
- Controller’s obligation to document data breach (Art. 15 para. 4 nFDPO)
- Processors must notify controllers "as soon as possible" (regardless of the risks involved)

Data Security (5|5)

Art. 8 and 24 FDPA; Arts 1–5 and 15 nFDPO

LAUX LAWYERS AG
ZURICH | BASEL

(1) Define clear tasks, responsibilities and competencies within your organization
→ Designate privacy and incident response leads

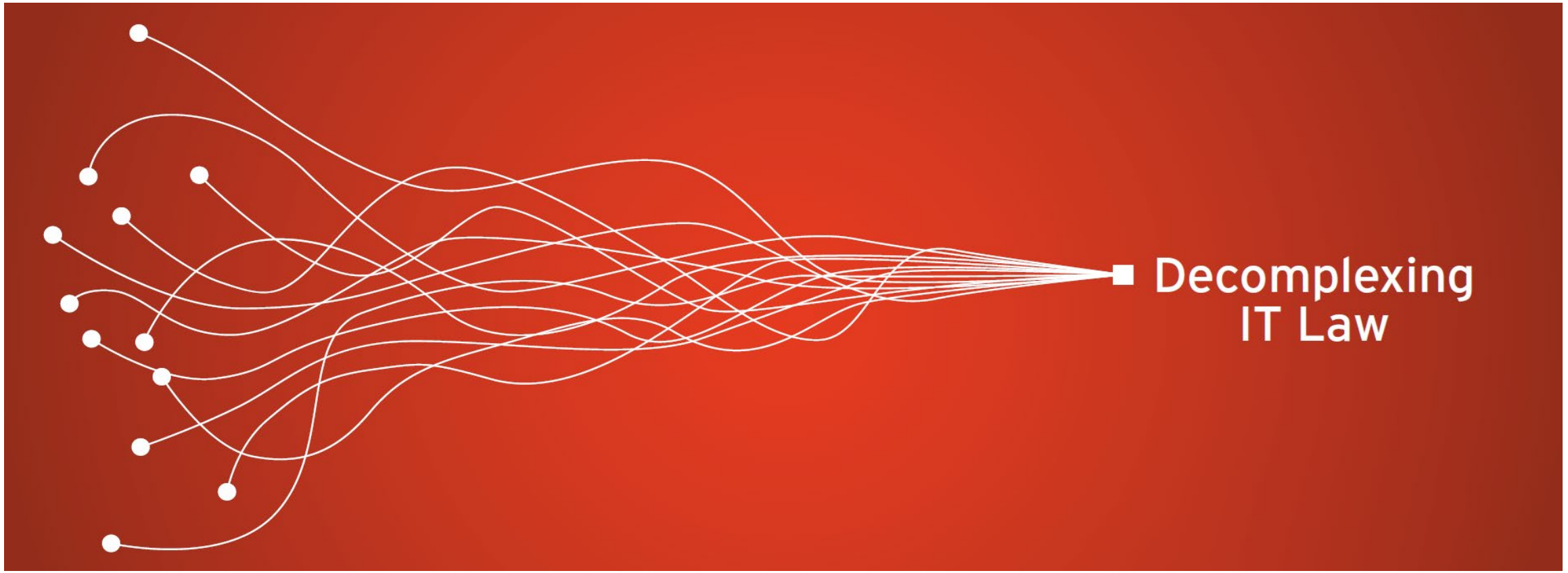
(2) Understand your data flows
→ How do you collect, store, share, protect, and dispose of (personal) data?

(3) Check your data practices against (other) applicable laws and regulatory requirements
→ Information security compliance is a broader topic than (personal) data security!

(4) Develop and implement compliant documentation
→ Review annually, audit and monitor, and provide training

(5) Conduct appropriate assessments (privacy, operational, and cyber risks)
→ As required by applicable law and in accordance with industry common practices

Focus Topic #2: Records of Processing Activities



Records of Processing Activities (1|2)

Art. 8 nFDPA; Art. 2 of the new Data Protection Ordinance (nFDPO)

LAUX LAWYERS AG
ZURICH | BASEL

Key questions when implementing data protection compliance

- What personal data does the company process, about whom, and for what purposes?
- From what sources does the company receive or collect the personal data?
- To whom does the company disclose the personal data?
- For how long does the company hold the personal data
- How does the company keep the personal data safe (data security)

How to find out and document?

- *IT professionals* are ideally situated to provide or gather the facts (supported by Information Governance and Legal and Compliance)
- Draw information from your list of applications
- Categorize by business process
- Document findings in *Records of Processing Activities*

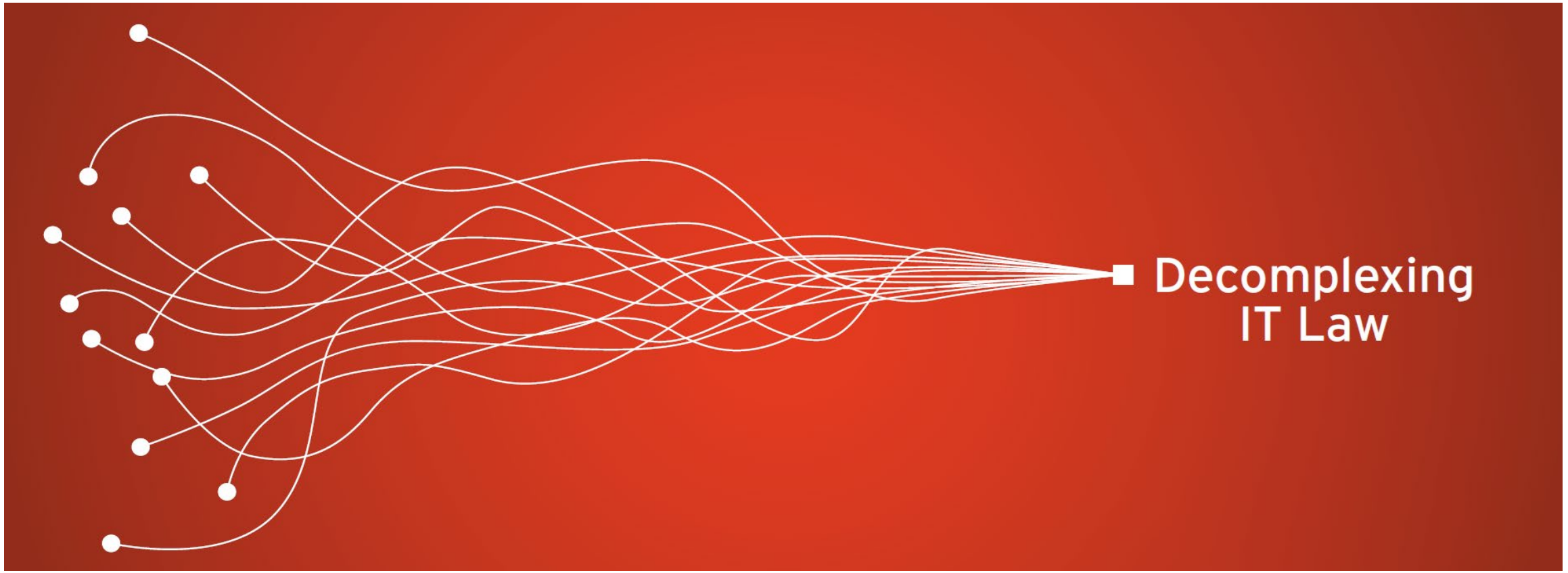
Records of Processing Activities (2|2)

Art. 12 nFDPA; Art. 24 nFDPO

	A	B	C	D	E	F	G
1	Controller						
2	Name and contact details		Data Protection Officer (if applicable)		Representative (if applicable)		
3	Name		Name		Name		
4	Address		Address		Address		
5	Email		Email		Email		
6	Telephone		Telephone		Telephone		
7							
8	Article 30 Record of Processing Activities						
9	Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individual	Categories of personal data	Categories of recipients	Link to contract with processor
10							
11							
12							
13							

(Template provided by UK ICO, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/)

Focus Topic #3: Control over Service Providers (Outsourcing)



Control over Service Providers (1|4)

Art. 9 nFDPA; Art. 7 nFDPO

LAUX LAWYERS AG
ZURICH | BASEL

- External service provider performs your organization’s processing operations on the *instructions* of your organization (think: "extended workbench“; also: "contract processing")
- Your organization – being the "controller“ – remains responsible for compliance
- Art. 9 nFDPA: Your organization needs to enter into a written agreement with the external service provider – being the "processor" – to ensure that the service provider processes the personal data only as instructed, and guarantees to implement appropriate data security
- Privilege: disclosures to data processors do not qualify as disclosures to third parties (no justification required)

Control over Service Providers (2|4)

Art. 9 nFDPA; Art. 7 nFDPO

LAUX LAWYERS AG
ZURICH | BASEL

→ **Practical tips: vendor due diligence**

- Careful **selection, instruction and control** of service providers
- Data protection risk (and, potentially, impact) assessment in the procurement process
- Know and understand the measures and processes implemented by the service provider
- Review and optimize contractual safeguards
- Check and supplement your **own** technical and organizational security measures (note: "shared responsibility")
- Implement a process for regularly reviewing the effectiveness of the measures

Control over Service Providers (3|4)

Art. 9 nFDPA; Art. 7 nFDPO

LAUX LAWYERS AG
ZURICH | BASEL

→ **Practical tips: contract**

- Service provider's obligation (as processor) to follow your organization's instructions (as controller)
- Description of the subject matter and scope of the contract processing
- Obligation to implement a **data security** level commensurate with the risks for individuals
- Provisions ensuring your organization may **object to new sub-processors**
- **Information, cooperation and confidentiality** obligations of the service provider
- **Audit rights** of your organization (control during the term of the contract)
- Safeguards for professional secrecy obligations (if applicable)
- Safeguards for international data transfers

Control over Service Providers (4|4)

Art. 9 nFDPA; Art. 7 nFDPO

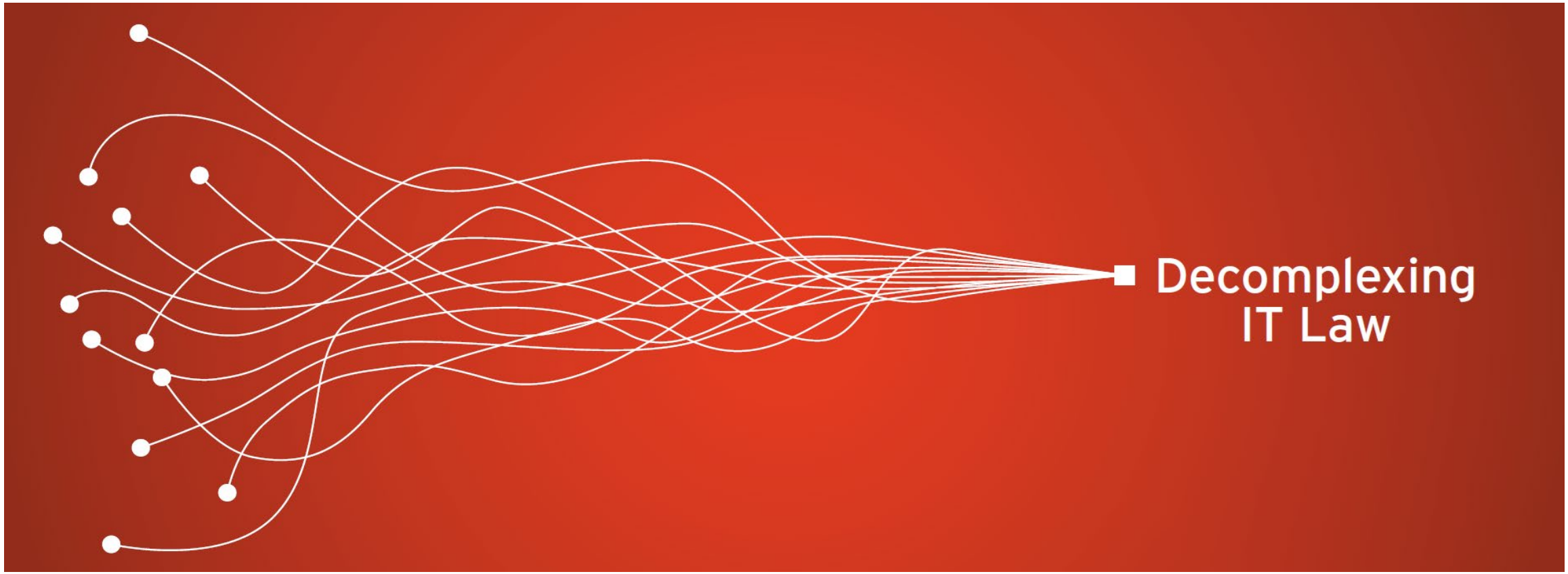
LAUX LAWYERS AG
ZURICH | BASEL

→ **Practical tips: data security**

- Ensure service provider (processor) will implement adequate measures to prevent data breaches
- Your organization (controller) may rely on robust documentation from the service provider regarding technical and organizational data security measures
- Certification in accordance with ISO standards can be a suitable documentation to prove sufficient data security measures are implemented
- Increased trustworthiness: if service provider makes available reports from data security audits

Questions and Discussion

LAUX LAWYERS AG
ZURICH | BASEL



Contact

Thomas Steiner

Dr. iur., LL.M., Attorney at Law, Senior Advisor/Partner

@ thomas.steiner@lauxlawyers.ch

w www.lauxlawyers.ch

n linkedin.com/in/thomassteiner1

LAUX LAWYERS AG

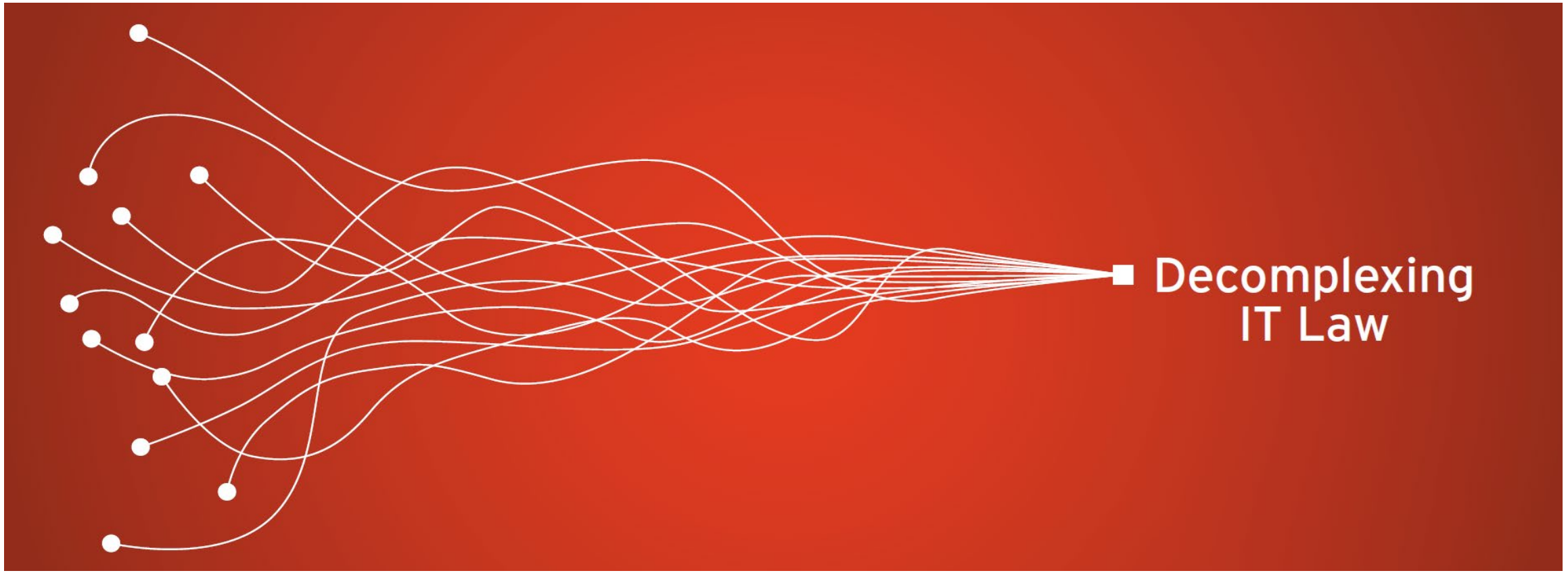
Schiffbaustrasse 10

P.O. Box

8031 Zurich

+41 44 880 24 24

Annex: nFDPA Implementation Check List



nFDPA: Implementation Measures (1|2)

Requirements		Implementation
	– Processing principles (esp. data minimization, and storage limitation)	– **Know your data and processing operations!** *Key questions: What personal data does the company process, for what purposes and in what roles? From whom does the company receive the personal data? How long does the company store the personal data and how is it protected?*
	– Documentation	– **Records of Processing Activities**
	– Data subject rights	– **Internal Data Protection Policy** (principles, responsibility, data protection contact; process descriptions)
	– Transparency (Duty to inform)	– (General) **Privacy Notice** (addressing customers, and contacts at customers, suppliers or other business partners; website users) – **Employee Privacy Notice**

nFDPA: Implementation Measures (2|2)

Requirements		Implementation
	– Data security (appropriate to risks for data subjects)	– Implement and document **technical and organizational measures (TOM)**
	– Data breach notification	– **Process description** for handling data breaches (internal investigation, notification to authorities and/or data subjects)
	– Control over service providers (outsourcing)	– Careful **selection, instruction and control** – **Data processing agreements**
	– Safeguards for inter-national data transfers	– Identify international transfers (internal fact finding) / safeguard transfers to non-adequate import countries / Safeguards: **Standard Contractual Clauses**; Transfer Impact Assessment