Digitalisation process: from electronic signature to archiving

Presentation by **Audrey Rustichelli and Nicolas Hamblenne**
8 June 2021

pwc | PwC Legal

1

Introduction

“Digital” Workshop Series

“Digital” Workshop Series

How to prepare for digitalisation

Electronic signatures

14th June 2021

Digitalisation and archiving of documents

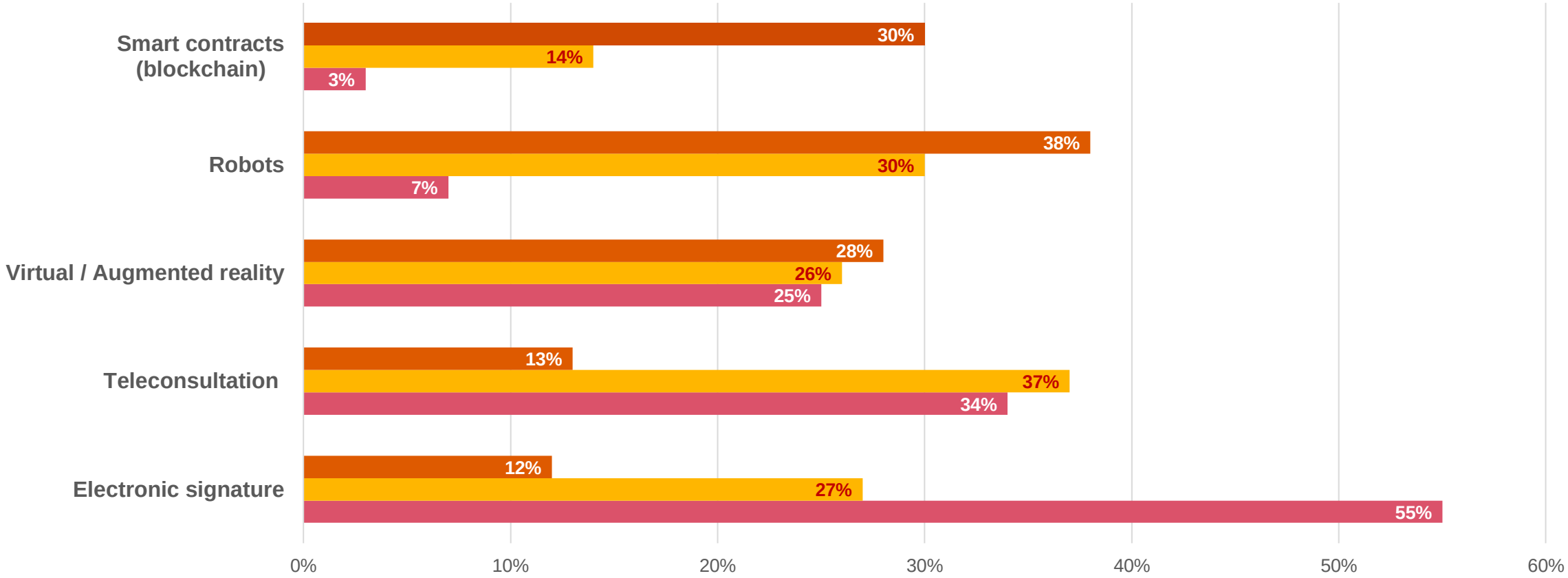
21st June 2021

Digitalisation in the insurance sector

What is digitalisation in concrete terms ?

- Digital portals for brokers and customers
- Online subscription of services
- Electronic signatures
- Chatbots
- Online management of claims
- SEO
- Artificial intelligence
- (Real) use of CRMs
- Better flow of information, seamless experience for the customer
- Digital archiving, cloud computing
- Insurtechs / use of blockchain
- etc

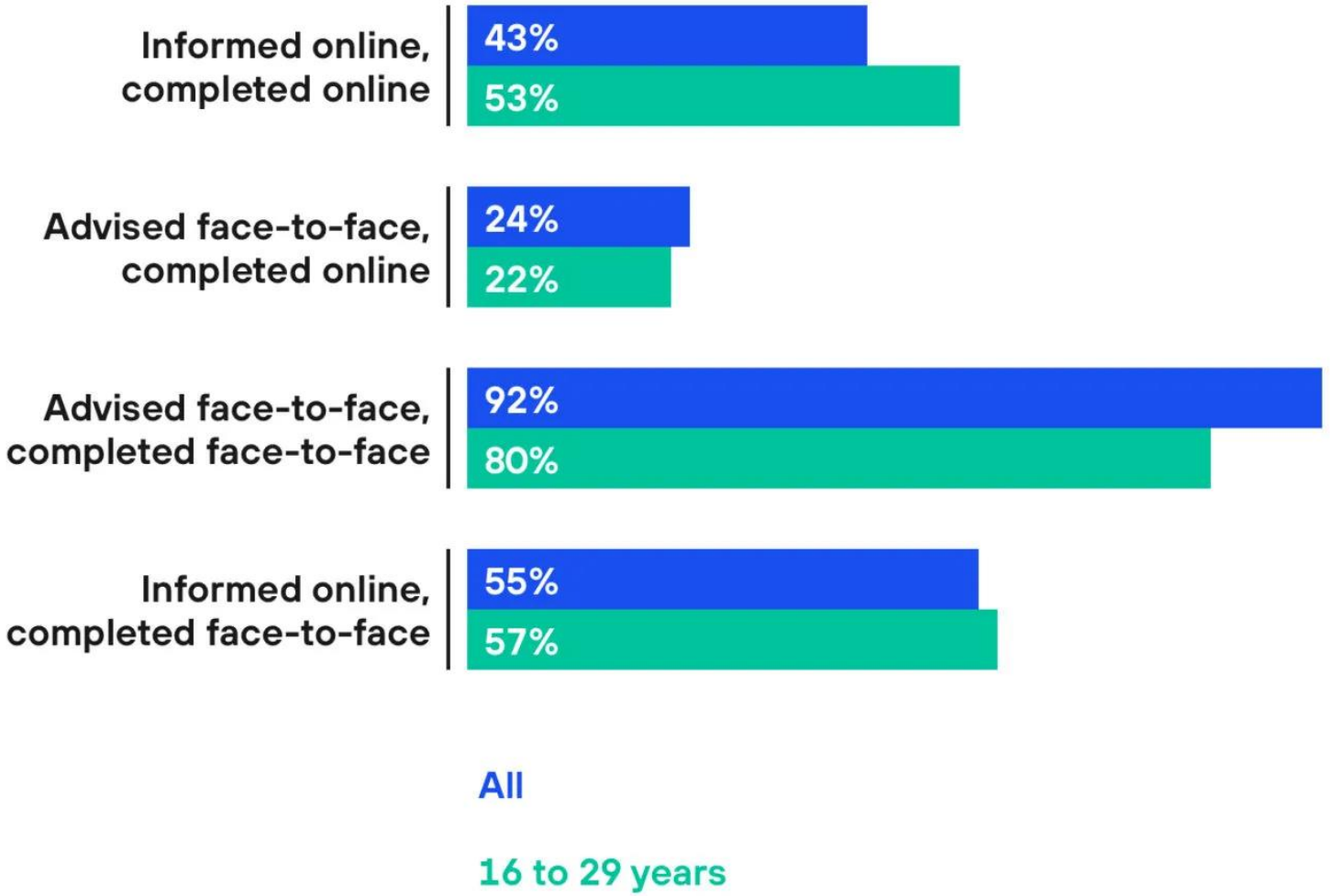
Have the following technologies already been integrated into the customer journey ?

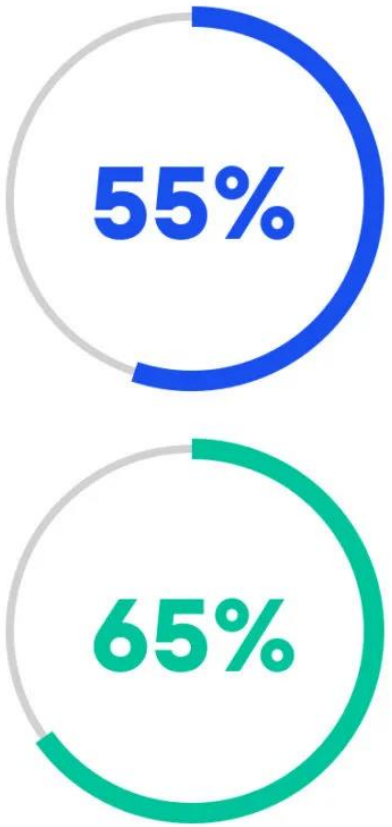


Source : CXP Group : l'innovation numérique, enjeu clé de l'assurance pour 2020

Every second person has at some time taken out an insurance policy online

In which way did you conclude your insurance policies in the past?





Source: Bitkom Research 2019 (www.bitkom.org)

2

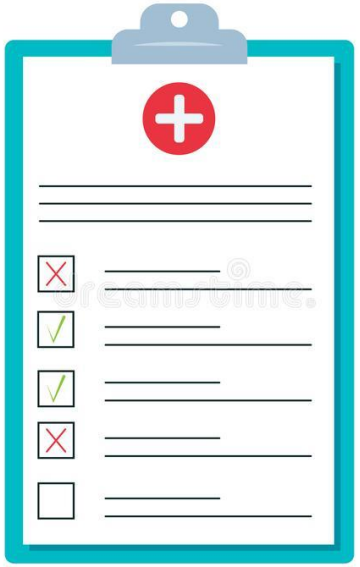
How to prepare for digitalisation

“

The reality is, many digital transformations fail because companies aren’t integrating their business and technology strategies from the start.

Chris Bedi,
CIO of ServiceNow

Introspection



Explore your own organisation

- What documents are you currently using?
- What are your current processes (onboarding, renewals, termination, etc)?
- What steps must a customer follow before enjoying a service?
- Is it efficient? What are my current challenges and what do I need to improve?
- Etc.

Legal Due Diligence / Asking yourself key questions

QUESTION 1

Should our documents be (i) accepted, (ii) signed or (iii) neither ?

When is a signature legally mandatory?

Requirements for valid contracts

For <u>most</u> contracts:

1. Consent to essential elements of the contract (e.g. via “opt-in”)
2. Legal capacity
3. Valid subject-matter
4. Valid cause

But…… certain legal provisions, regulations or guidance require a signature on some specific documents

Obligation to sign

➢ **Law on insurance contracts**

- amendment agreement for the transfer of an insurance life contract (Article 199§1)
- agreement signed by policyholder, the insurer and the pledgee if an insurance contract is pledged. The beneficiary who has accepted the benefit of the contract must also consent to such pledge (Article 117)
- amendment agreement to the insurance policy for the beneficiary to accept the benefit of the contract (Article 122). The beneficiary, the policyholder and the insurer must sign such agreement.

➢ **Guidance from the CAA**

Evidence : How to enforce contractual obligations?

How to prove validity in case of litigation?

Written evidence principle: need for

1. A notarised deed; or

2. A private agreeement (i.e. written & signed incl. electronically)

Exemptions to principle:

1. Value of contract below EUR 2,500
2. Litigation between traders=any means of evidence accepted
3. Party has *prima facie* evidence (e.g. email, invoice, unsigned document) and other evidence (witness and/or presumptions)
4. Contractual derogations or variations by the parties

Insurance sector

Article 16 of the law on insurance contracts:

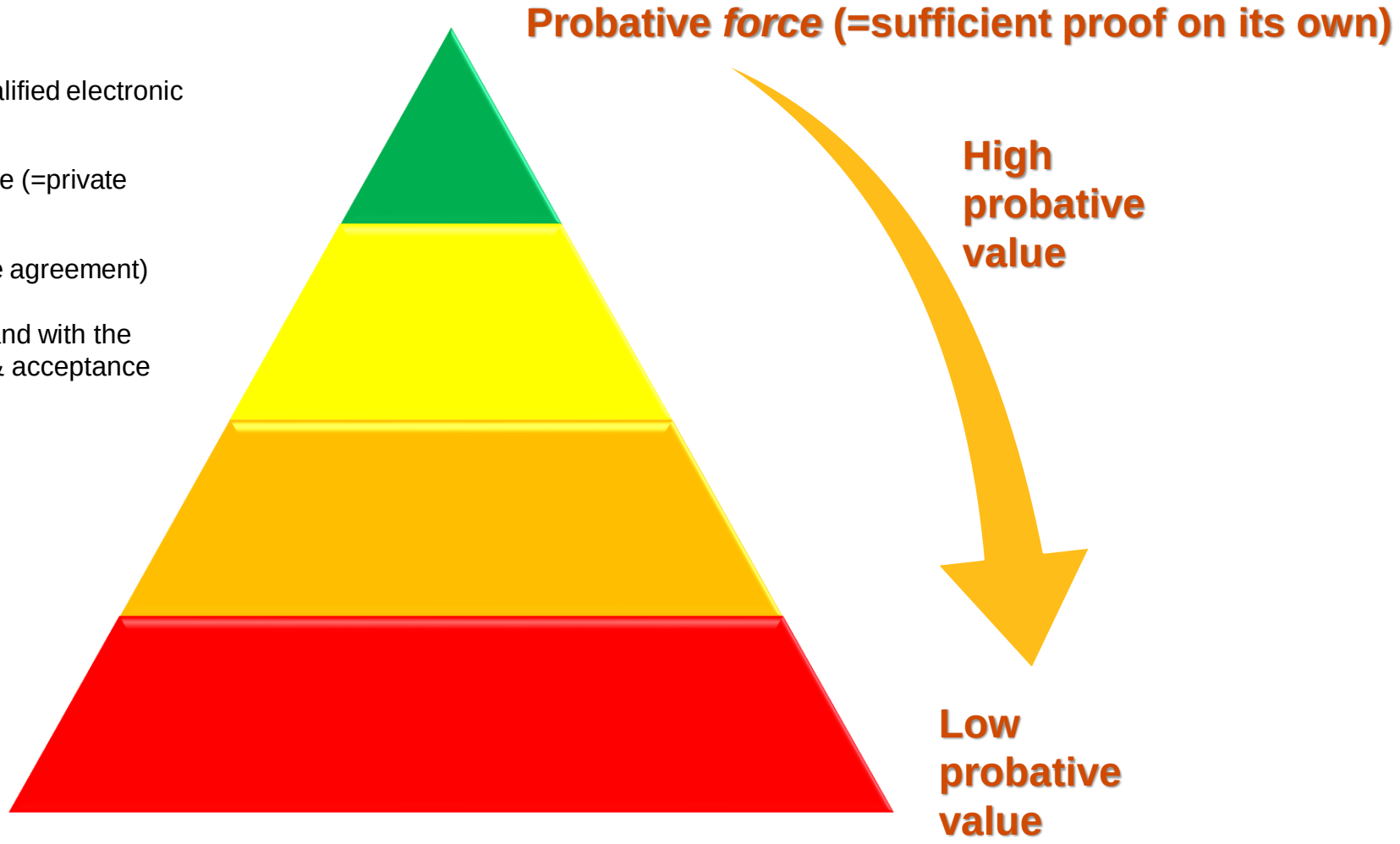
"With the exception of admissions and sworn statements, and irrespective of the value of the commitments, the insurance contract as well as its amendments are proved between parties **in writing**. No witness or presumptive evidence against the content of the act is admitted."

Article 62-8 of the law on insurance contracts

For contracts concluded remotely (e.g. via a web platform), the insurer bears the burden of proof notably in respect of the policyholder's consent to enter into the contract

Evidence : Not all evidence is equal!

- Notarised deed (*acte authentique*)
- Document with a handwritten signature or a qualified electronic signature (=private agreement)
- Document with an advanced electronic signature (=private agreement)
- Document with an electronic signature (=private agreement)
- Document accepted via an electronic platform and with the possibility to prove the reliability of the system & acceptance
- Copy of signed documents sent by fax
- Copy of signed document sent via post
- Copy of document with a scanned signature affixed thereto
- E-mail with proof of receipt / Documents & data stemming from an IT system (e.g. SAP)
- Invoice / account statement without signature (sent by non-registered post)
- E-mail without acknowledgement of receipt



Signed or accepted? Main take-aways

1. Signatures are not always necessary for contract validity.

2. Companies will be able to prove validity by any means of evidence (e.g. logs, emails, witness) for B2B contracts.

3. A signed contract is however easier in case of litigation and companies need to retain sufficient evidence of validity.
4. When a signature is neither necessary nor highly useful to enter into an agreement, one can obtain the counterparty's consent (incl. online) to the agreement
   - a contract concluded by such electronic acceptance can only amount to prima facie evidence (*commencement de preuve par écrit*) as opposed to a private agreement (*actes sous seing privé*)
   - the party on which the burden of proof lies (i.e. the insurer in respect of the contract's existence and amendments thereto) has to be able to evidence the counterparty's acceptance on the essential elements of the contract for a judge to acknowledge the existence of a contract
5. Prudent approach to be adopted if multinational elements present

Legal Due Diligence / Asking yourself key questions

QUESTION 2

Are there any legal hindrances to digitalisation?

Any legal hindrances to digitalisation?

- **Remote conclusion of insurance contracts – A show stopper or a mere constraint?**
  - Definition of “remote conclusion of contracts”
  - Timing of conclusion
  - Communication of information before being bound by a remote contract
  - Consumer has a right to request information on paper

- **IDD - Digital process needs to take into account additional constraints**
  - Duty to advise
  - Additional paperwork (KID – IPID)
  - Difficulties for complex and structured products
  - Client consent / personalised online space?
  - Paper document or durable medium (under specific conditions)
  - No uniform EU implementation

Any legal hindrances to digitalisation?

- **KYC**
  - KYC may be a challenge in a full digital environment
  - Identification via electronic signature?
  - Personal platform to upload documents

- **Check ID cards online?**
  - Almost never fully digitalised
  - Luxtrust certificate?
  - New e-Wallet proposition of the EU Commission (European Digital Identity)

Legal Due Diligence / Asking yourself key questions

Question 3

If a signature is required:

- can it be signed electronically?
- If yes, which type of electronic signature should be used (simple vs advanced vs qualified) ?

Session 2

Question 4

How should the signed documents be kept ?

What safeguards should be put in place to keep the probative value of digital documents ?

Session 3

3

Conclusion

Questions ?

Thank you for your attention

Me Audrey Rustichelli
T: +352 26 48 42 35 98
E: audrey.rustichelli@pwclegal.lu

Me Nicolas Hamblenne
T: +352 26 48 42 35 58
E: nicolas.hamblenne@pwclegal.lu

www.pwclegal.lu

Digitalisation process: from electronic signature to archiving

Presentation by **Audrey Rustichelli and Nicolas Hamblenne**
14 June 2021

pwc | PwC Legal

“Digital” Workshop Series

How to prepare for digitalization

8th June 2021

Electronic signatures

14th June 2021

Digitalisation and archiving of documents

21st June 2021

Main takeaways of the previous session (digitalisation)

1. Digitalisation is a top priority for the insurance sector and it can take various forms (electronic signatures, chatbots, digital portals, etc).

2. Introspection is necessary before any digitalisation process.

3. Signatures are not always necessary for contract validity but it is often recommended to retain sufficient evidence of validity (useful in case of litigation).

4. Evidence is not always equal in terms of probative value (email vs wet-ink signature vs electronic signature).

5. Measures can diverge from country to country due to the nature of the legal instruments (directives, national laws)

1

Electronic signatures - Background

eIDAS (Regulation EU 2014/910) Trust and interoperability

- Creation of a harmonised and transparent legal framework across the EU
- Common security norms and standards
- Article 25 of the Regulation provides:
  - An **equivalence principle**
  - A **non-discrimination principle**
  - A **mutual recognition principle for qualified** electronic signatures across the EU
- Applicable in Luxembourg law since 01/07/2016

What is a signature?

Article 1322 of the Code provides that: "*The signature necessary for the conclusion of a private agreement identifies the one who signs and accepts the contents of the act. The signature may be handwritten or electronic.*"

Article 1322-1 of the Luxembourg Civil Code

- Identifies the signatory
- Demonstrates the signatory's adherence to the content of the document
- A signature is necessary to complete a private agreement *(acte sous seing privé)*
- A signature can be handwritten or electronic
- An electronic signature consists in a "*set of data, inseparably linked to the document, which guarantees its integrity and satisfies the condition of identification of the signatory and manifests his agreement with the content of the document*"

Article 1322-2 of the Luxembourg Civil Code

- An electronic private document (e.g. any contract/document) is valid as an original when it presents reliable guarantees as to the maintenance of its integrity from the moment it was first created in its final form

2

What are the different types of electronic signature?

e-Signature : 3 types of signatures not equal in case of litigation

Qualified electronic signature

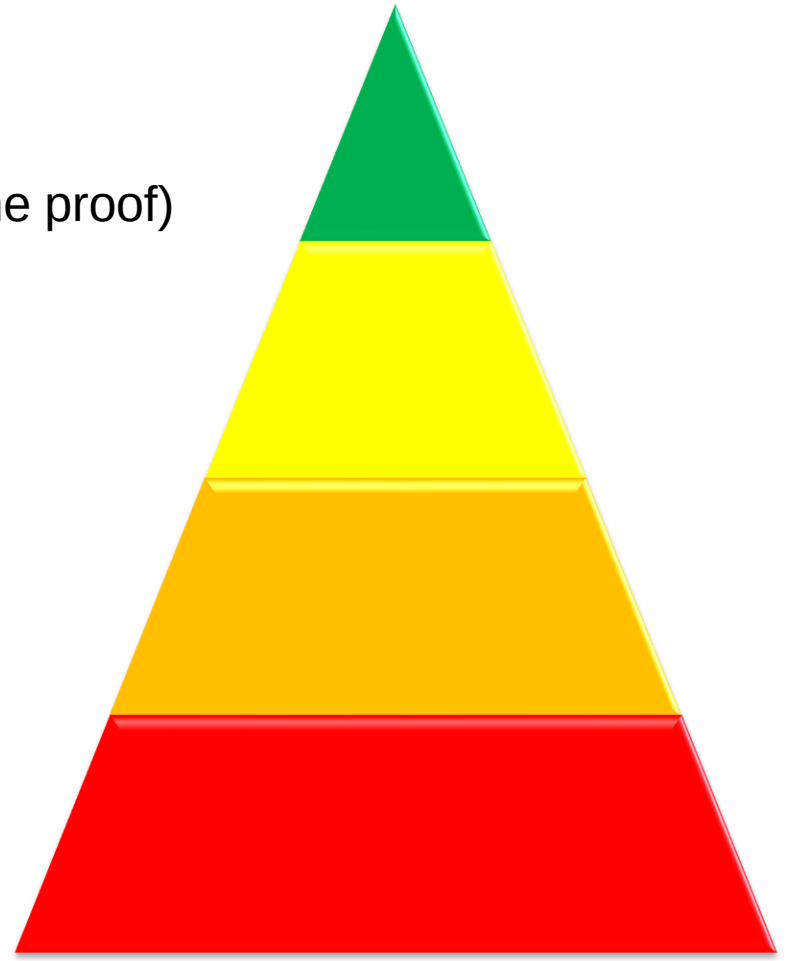
Deemed as equivalent to handwritten signature
(reversal of the burden of the proof)

Advanced electronic signature

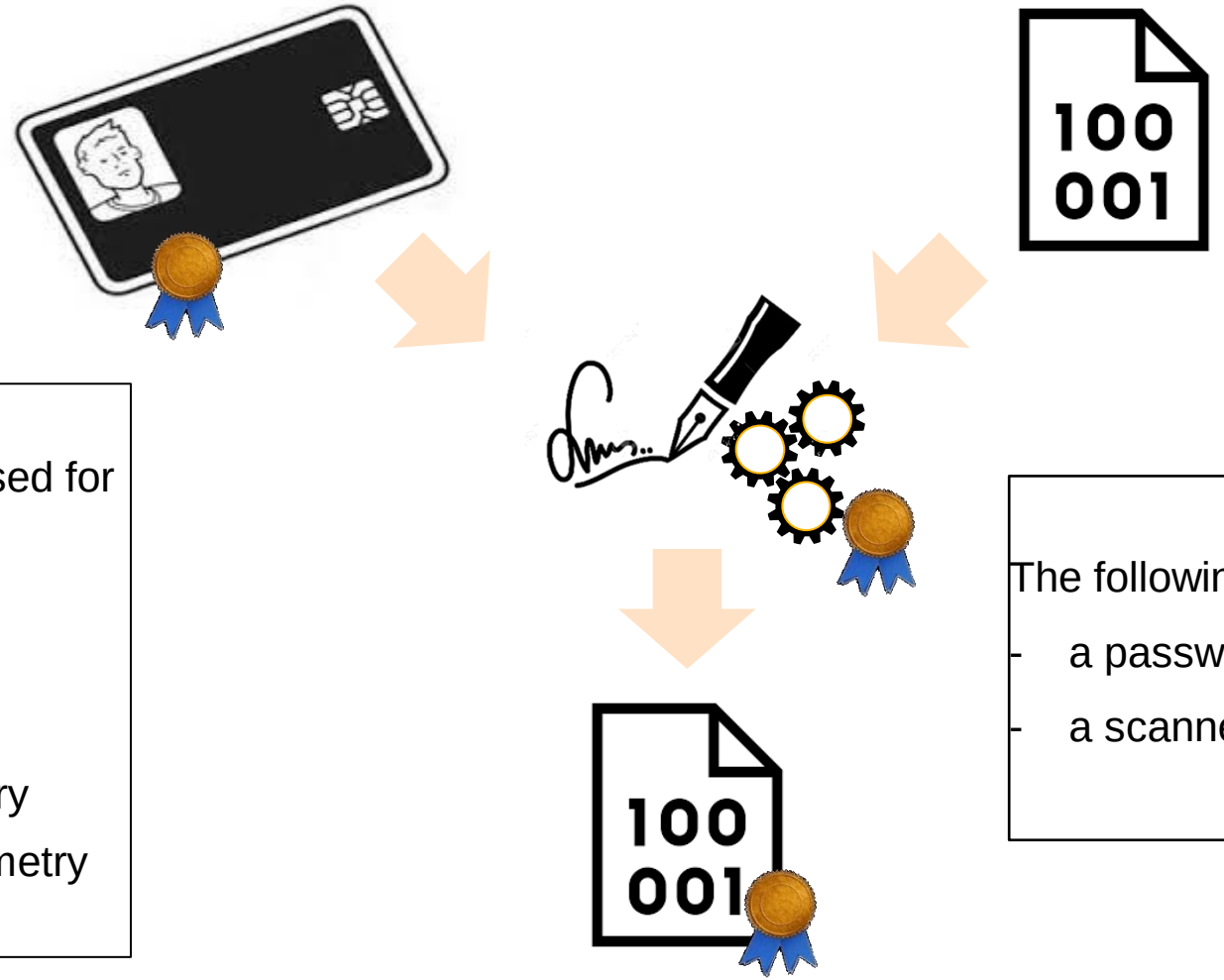
Party relying on signature needs to demonstrate that the requirements are met

(Simple) Electronic signature

Poor evidential value



In practice : how does it look like?



Devices commonly used for e-signatures:

- Token
- Smartcard
- Mobile App
- Tablet with biometry
- Tablet without biometry

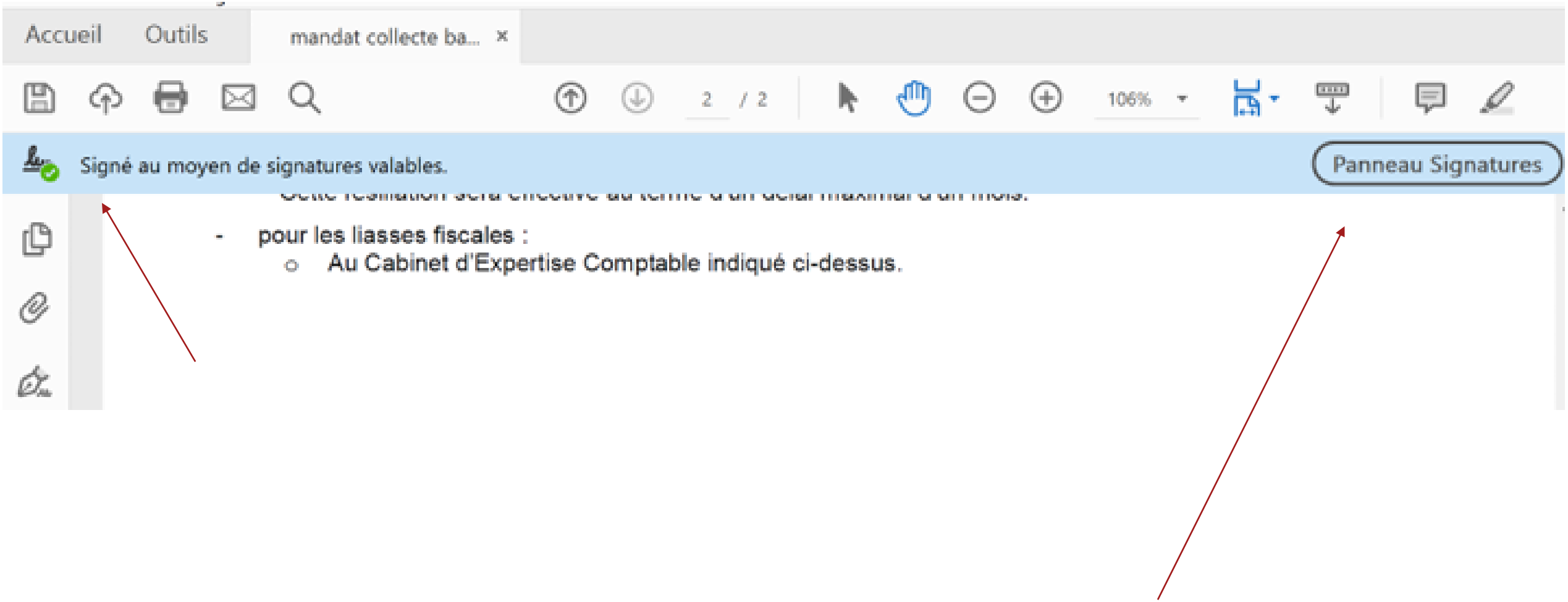
The following are not electronic signatures:

- a password entered onto a platform;
- a scanned copy of a handwritten signature

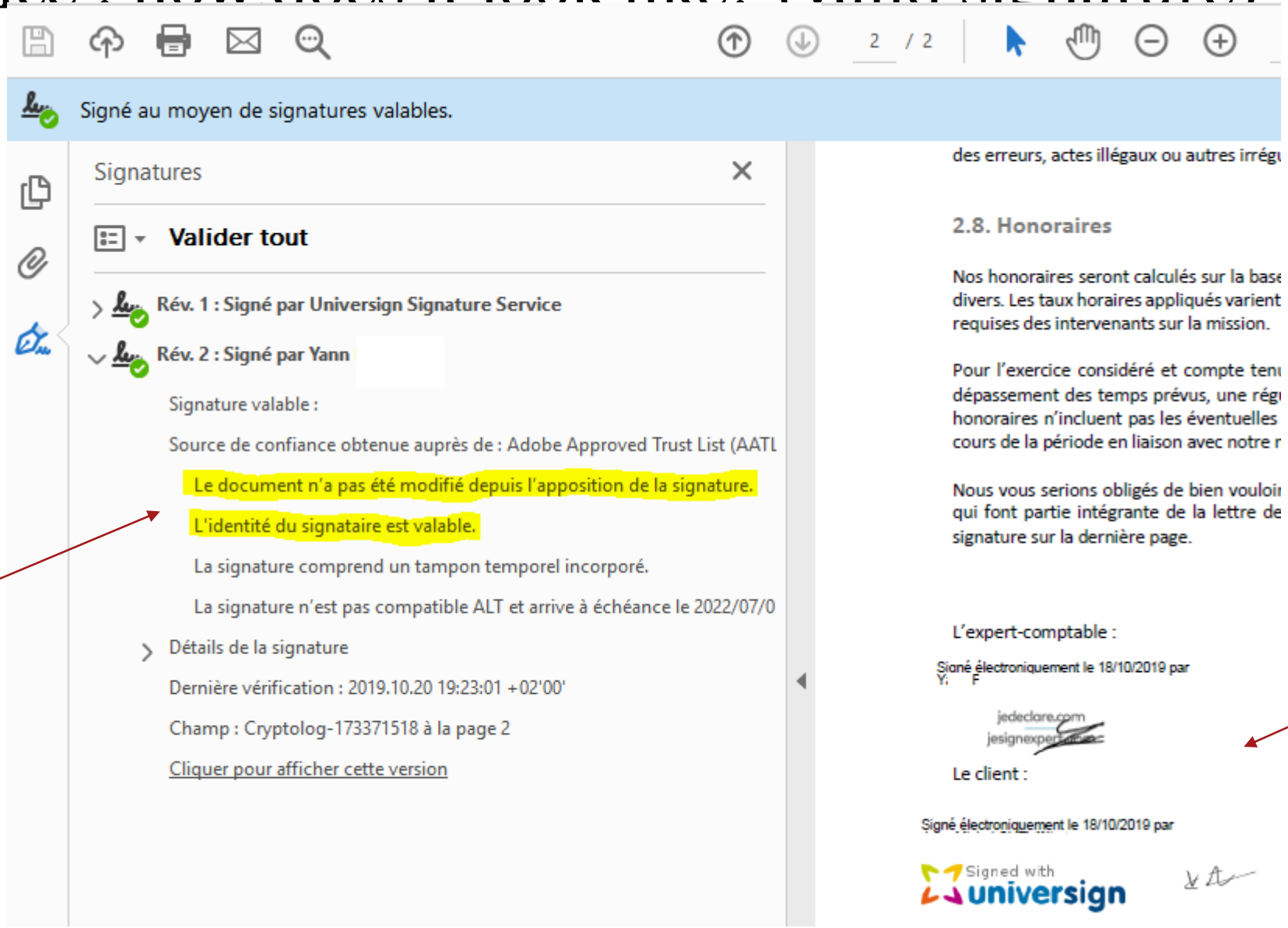
e-Signature : Different devices = different values

	Smart card	**GSM**	**Tablet *without* biometry**	**Tablet *with* biometry**	**Tokens**
Qualified eSignature	✓	✓			✓
Advanced eSignature		✓		✓	
(Simple) eSignature			✓		

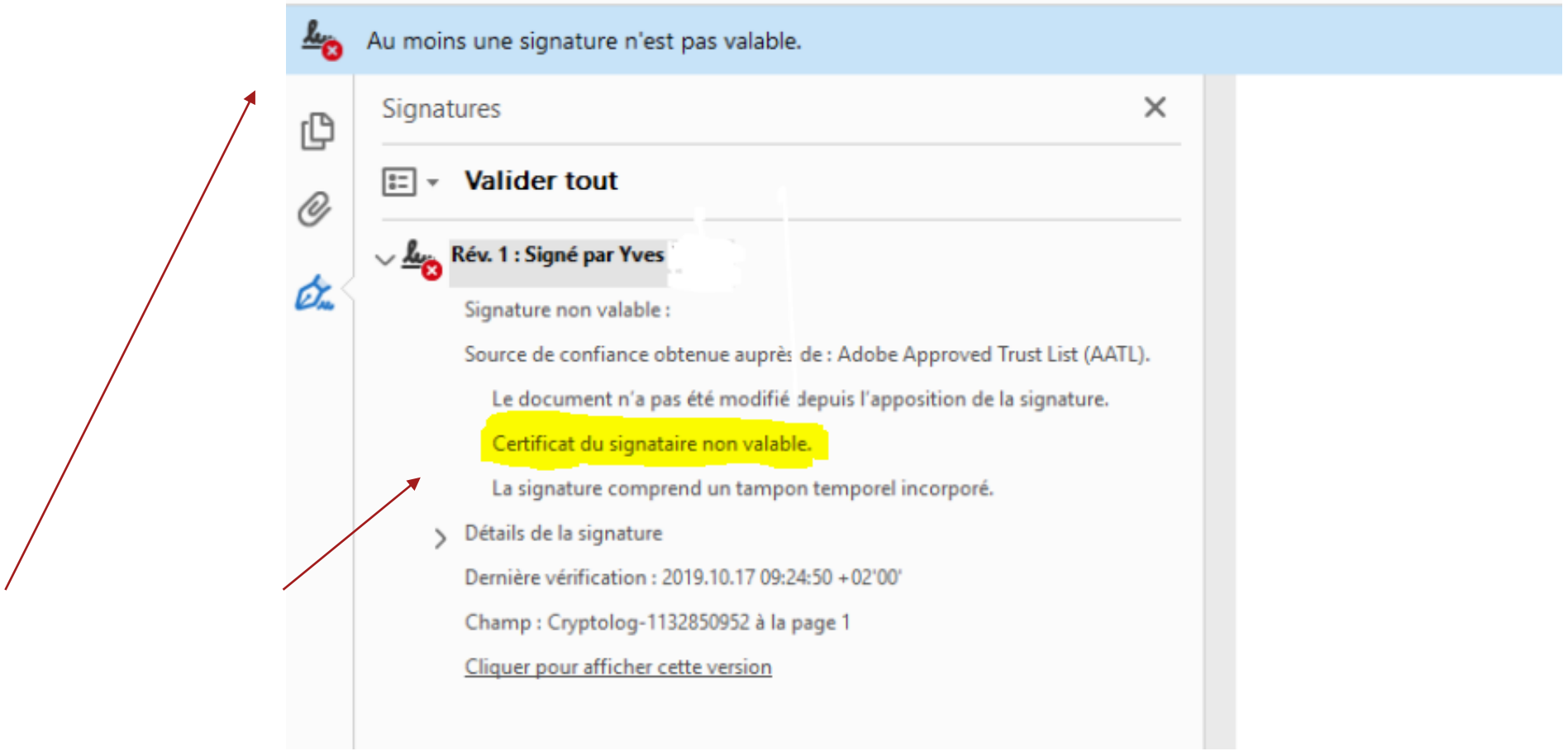
In practice : how does it look like?



In practice : how does it look like? (valid signature)



In practice : how does it look like? (invalid signature)



Advantages of electronic signatures and attention points

Advantages

- High level of security for qualified and advanced signatures
- Easy to implement
- No physical presence required
- Time and cost efficiency
- Documents immediately available to all signatories

Attention points

- Might be burdensome (qualified signatures)
- Exclusions where only handwritten signatures are allowed
- Probative value not always equivalent to handwritten signatures (but principle of non-discrimination)
- Archiving of documents signed electronically must be processed with caution
- Risks for global projects (non-uniform application of eIDAS regulations)

Which documents can be signed electronically?

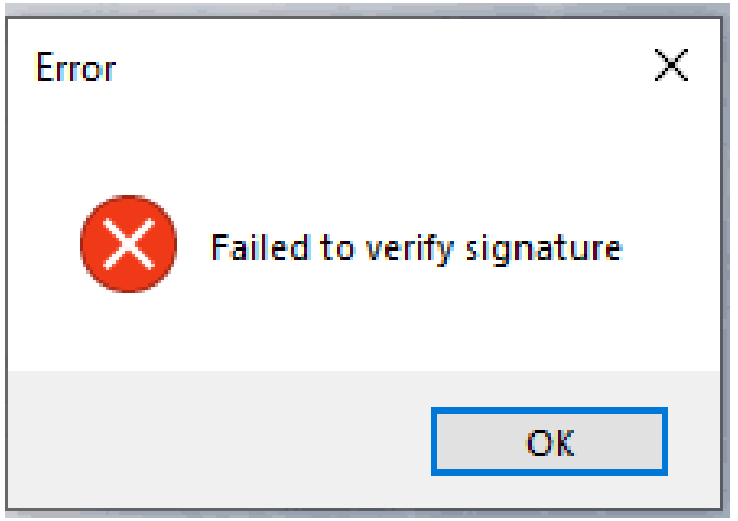
e-Signature: Can all documents be signed electronically?

Certain documents cannot be signed electronically:

- Notarised deeds
- Administrative acts (except if express authorisation, e.g. VAT declaration)
- Real estate sales contract
- Other documents due to sectoral rules or practices

Contracts with applicable laws and/or competent jurisdictions other than Luxembourg:

- In principle, only an issue when non-EU
- Prior clearance with local counsel needed



Documents that can be signed electronically

- **B2B & B2C Private agreements** can be signed either by handwritten signature or by an electronic signature:

- Insurance policies (life/non-life)
- Credit contracts
- Life insurance contract
- Investor profile
- Commercial contracts
- Board meetings
- Employees contracts
- ….

Costs/Benefits comparison

	Simple	Advanced	Qualified
Identification of the signatory	X	~	V
ease of installation and use	V	~	X

4

Specific questions

Can a company sign electronically?

Facts

In principle, NO (eIDAS's defition of "signatory" refers to a natural person who creates the electronic signature)

- **However**, individuals – with the power to represent the company – can sign a document that will be legally binding for their company if they signed on its behalf

Attention points

- persons must be able to bind the company
- persons with signing authority must be able to sign electronically

Can a minor sign electronically?

Facts

- In principle, YES

Attention points

- No Luxembourg law prohibiting the use of electronic signature by minors.
- Question of discernment/representation (age at which a minor can validly enter into a contract alone)

Next steps?

Archiving

How should the signed documents be kept ?

What safeguards should be put in place to keep the probative value of digital documents ?

For how long should you keep the documents signed electronically ?

Session 3

3

Conclusion

Questions ?

Thank you for your attention

Me Audrey Rustichelli
T: +352 26 48 42 35 98
E: audrey.rustichelli@pwclegal.lu

Me Nicolas Hamblenne
T: +352 26 48 42 35 58
E: nicolas.hamblenne@pwclegal.lu

www.pwclegal.lu

Digitalisation process: from electronic signature to archiving

Presentation by **Audrey Rustichelli and Nicolas Hamblenne**
21 June 2021

pwc | PwC Legal

“Digital” Workshop Series

How to prepare for digitalization

8th June 2021

Electronic signatures

14th June 2021

Digitalisation and archiving of documents

21st June 2021

Main takeaways of the previous sessions (digitalisation and electronic signatures)

1. Digitalisation (including electronic signatures) is a top priority for the insurance sector.

2. Introspection is necessary before any digitalisation process.

3. Signatures are not always necessary for contract validity but it is often recommended to retain sufficient evidence of validity (useful in case of litigation).

4. There are 3 different types of electronic signatures (simple/advanced/qualified), they do not have the same strenght in terms of probative value (only the qualified is presumed to be equivalent to handwritten signature).

5. Not all documents can be signed electronically and for the ones that can be, it is a case-by-case analysis (risk-based approach).

6. Measures can diverge from country to country due to the nature of the legal instruments (directives, national laws).

1

Archiving - Background

Why archiving documents?

Concrete example of legal obligations to keep documents for a specific period of time

- e.g. Law of 12 November 2004 on the fight against money laundering and terrorist financing (art. 3)

"***Professionals shall be required to keep documents, data and information*** *(...)*

(a) ***with regard to due diligence measures*** *(...) (including, where appropriate, data obtained through the use of electronic means of identification, relevant trust services provided for in the* ***eIDAS Regulation*** *(...)* ***for five years*** *after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis; (....)*

b) ***information on the measures taken to identify the beneficial owners*** *(...)* ***for five years*** *after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis (Act of 25 March 2020)*."

Archiving in Luxembourg

Concrete example of legal obligations to keep documents for a specific period of time

- Article 1322-2 of the Luxembourg Civil Code

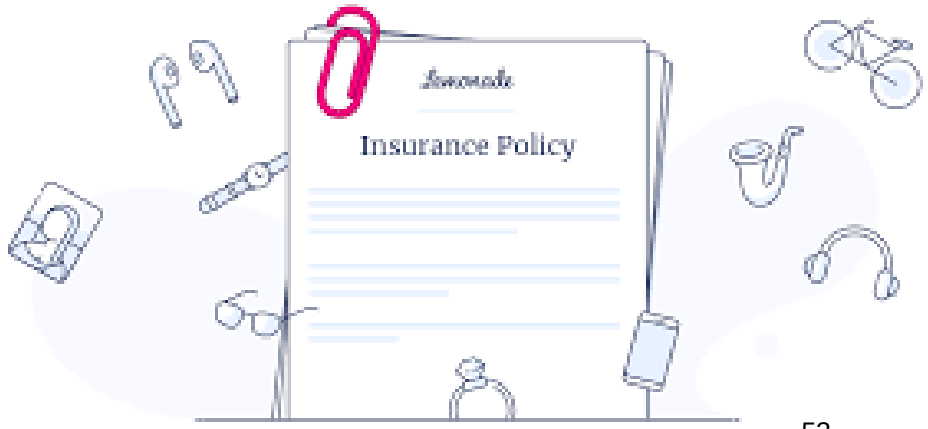
"***The electronic private document is valid*** *as an original* ***when it presents reliable guarantees as to the maintenance of its integrity*** *from the moment it was first created in its final form*."

- Law of 27 July 1997 on insurance contracts
- Law of 25 July 2015 on electronic archiving
- Grand-Ducal Regulation of 22 May 2017
- Law of 17 August 2018 on archiving

Concrete examples of retention periods for the insurance sector

Concrete example of legal obligations to keep documents for a specific period of time

- Criminal records (from candidates) : should be deleted **maximum 1 month** after the conclusion of the employment contract and **without delay** if the person concerned is not hired (Article 8-5 of the law of 23 July 2016 on the reorganisation of the criminal record)
- Insurance policy : **10 years from the termination of the insurance policy** (Article 44 of the Law of 27 July 1997 on insurance contracts) - no legal obligation, it is a recommendation based on the limitation period ("*prescription*")
- **Case-by-case analysis** (different scenarios in LIFE/NON-LIFE)
- Compare with your **record of processing activities** (GDPR)



Good practices in terms of archiving

Examples

- Appointing a “**Records Manager**”
- Complying with **ISO standards** (quality management : ISO 9000; information security : ISO 27000; etc) helps to set retention periods and measures to put in place for an efficient archiving
- **Risk of complaints and litigation procedures** (“*litigation hold*”) will usually be added to the legal retention period
- **Guidelines** issued by authorities, administrations and professional associations, certification standards
- Identify **legal/regulatory/contractual/business obligations** to keep documents (and the retention period as well as the “**trigger event**”)

2

How can you keep the probative value of digitalised documents?

Dematerialisation and preservation service provider ("PSDC")

PSDC

- **Certification by ILNAS**
- **PSDC must provide information** relating to the **conditions for dematerialisation or electronic conservation** for which it has been certified
- PSDC is bound by **professional secrecy**
- Art. 1334-1 : "***Digital copies that are created by a PSDC shall have***, *unless proven otherwise,* ***the same probative value as the original document*** *or as the document deemed equivalent to the original.*

  A copy cannot be dismissed by the judge *only because it is electronically presented or because it has not been created by a PSDC*."

Dematerialisation and preservation service provider ("PSDC")

PSDC

- **E-archiving allows documents to keep their probative force/value :**

➢ digital originals (including electronically signed documents) must be durable

➢ presumption of durability (no alteration possible and provided that the computer document has been securely created and electronically signed)

- Possibility to prove the evidential value of a document even if the archiving has not complied with the conditions of the law or has not been carried out via a PSDC (but such proof is more difficult)

Comparative overview (multi-jurisdictions)

Question	Luxembourg	France	Belgium
How can an insurance company take steps to ensure that the digitized Documents do not lose in probative value?	**High level answer**: Using a certified electronic archiving provider (Prestataire de services de dématerialisation et de conservation or "PSDC") to store the Documents is recommended. **Additional comments**: Using such a provider is important for sensitive documents (i.e. involving large sums or likely to cause litigation). If using such a provider is not possible, implementing appropriate measures safeguarding the Documents' integrity internally is recommended. For Documents that are accepted online but not signed, we recommend to keep evidence.	**High level answer**: no local equivalent to PSDC. Using a Luxembourg certified electronic archiving provider is possible subject to conditions. **Additional comments**: In order to facilitate proof of compliance, insurance companies should ask the Luxembourg provider to comply with the AFNOR NF Z42-013 and ISO 1464-1 standards. If using such a provider is not possible, implementing appropriate measures safeguarding the Documents' integrity internally is recommended. For Documents that are accepted online but not signed, we recommend to keep evidence.	**High level answer**: Using a PSDC, as such providers are regulated under Belgian law, to store the Documents is recommended. Using a Luxembourg PSDC could be problematic. **Additional comments**: Using such a provider is important for sensitive documents (i.e. involving large sums or likely to cause litigation). If using such a provider is not possible, implementing appropriate measures safeguarding the Documents' integrity internally is recommended. For Documents that are accepted online but not signed, we recommend to keep evidence.

Challenges of (e-)archiving

Challenges

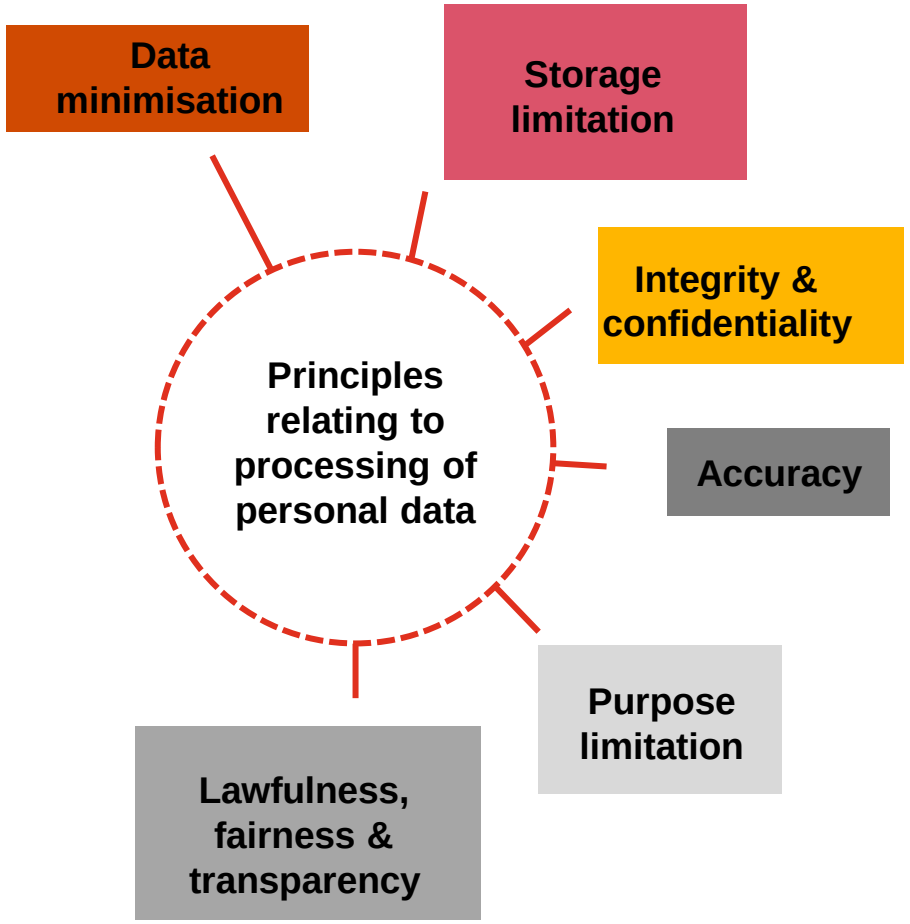
- Once the archiving period is set, this must be translated into **concrete actions** (operational process in place)
- "**Shadow IT**" (some documents are retained on personal drives / email boxes)
- **Change of operating systems and software tools** (challenge to keep track of all archives on a long term basis)
- **Software can complicate archiving** (no possibility to delete documents/information)
- Physical archiving **takes a lot of place** (km^2) and can be **costly**
- Digitalisation process **can destroy the probative force** of a document (e.g. document with a wet-ink signature that is scanned)
- Same for e-signed documents that are archived in paper (they lose all probative force, in particular if signed with a qualified signature)
- **Retention period** are often unclear
- **GDPR constraints**

3

GDPR aspects of archiving

Key principles

"The controller shall be responsible for, and be able to demonstrate compliance with the principles governing personal data processing"



Retention period

Longer retention period tolerated if :

- Public interest archiving purpose
- Scientific research
- Historical research

Provided that appropriate technical and organisational measures are in place.

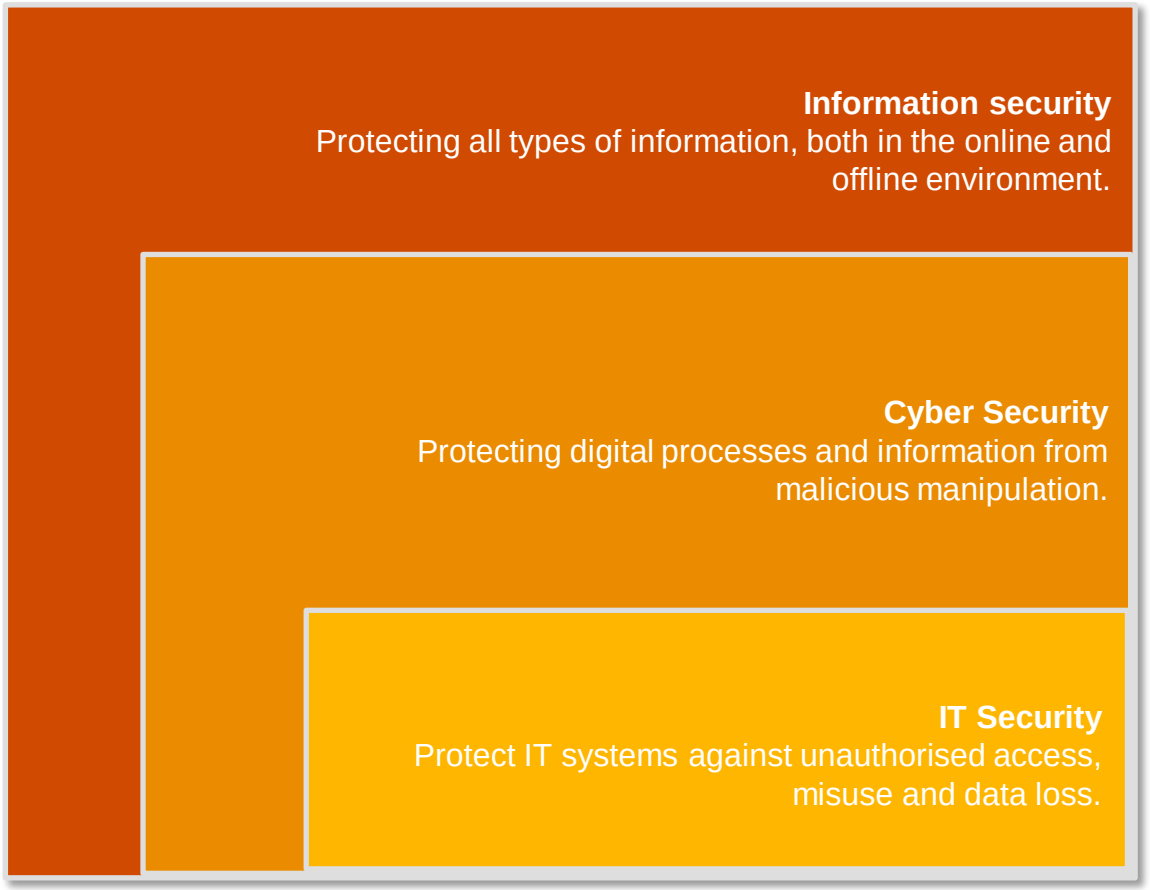
Is there a legal or public interest obligation (e.g. AML/KYC) to retain this data?

If not, what is the reason for the entity to keep this data?

Does the entity have measures in place to monitor compliance with the defined retention periods?

The retention periods for personal data must be defined internally.

Data security



Appropriate safeguards must be applied in relation to the personal data in question

- Inadequate data security can lead to heavy fines and reputational damage
- Pseudonymisation ≠ anonymisation

The GDPR does not apply to truly anonymous data

Key takeaways for (e-)archiving

- **Set-up retention periods**
- **Design internal processes for e-archiving** (as well as the “trigger event”) and try to **automate** it
- If you have a lot of documents to archive **select a sample** to see if documents can be either deleted/archived
- **Monitor “shadow IT”** and **raise awareness** within your companies
- **Archive regularly at multiple locations** to reduce the risk of loss (fire, floods, IT shortage, stealing, etc) and protect it **with appropriate measures** to avoid data breach (encryption, passwords, etc)
- **Set access rights** to relevant persons only (“need to know basis”)
- If you **are sub-contracting** the archiving process, assess the measures put in place by the processor (e.g. cloud provider) and sign a data processing agreement compliant with article 28 GDPR

Last reminders and quick tips

- **Archiving ≠ backup**
- **Pseudonymisation ≠ anonymization**
- Be careful if you decide to delete the information (it can often be restored from IT tools) **Physical destruction of documents and hardware is often recommended**
- **Clean desk policy** and **document shredders** (in particular for physical documents)
- **Privacy by design & by default** in order to have the minimum documents/information to archive
- Having an **internal policy/employee handbook** can be helpful (with a **table of retention periods**)

4

Specific questions

Is the retention period different between paper and electronic documents?

Answer

In principle, NO because the law is technology-neutral.

Attention points

- Be careful with the validity of electronic documents (validity of such documents can expire after a few years whereas the validity of handwritten documents usually remains).

In case of data subject access request, do I have to include the data that is archived?

Answer

In principle, YES

Attention points

- DSAR are complex in practice – set-up an internal policy to help employees managing such requests
- Some exemptions may apply (e.g. if delivering such information infringes the rights of a third party, etc).
- Documentation of process is also important in case you have deleted the information (to demonstrate to the data subject that his/her data have been deleted).

3

Conclusion

Questions ?

Thank you for your attention

Me Audrey Rustichelli
T: +352 26 48 42 35 98
E: audrey.rustichelli@pwclegal.lu

Me Nicolas Hamblenne
T: +352 26 48 42 35 58
E: nicolas.hamblenne@pwclegal.lu

www.pwclegal.lu