



How GDPR helps you master your KYC digital risk

Sylvie Dessolin

Senior Consultant
Sopra Steria Consulting
Luxembourg

Lucas Colet

Lead Security Manager
Sopra Steria Consulting
Luxembourg

Stéphane Badey

Partner
Arendt Regulatory &
Consulting

Bénédicte d'Allard

Manager
Arendt Regulatory &
Consulting

The speakers



Sylvie Dessolin
Senior Consultant
Sopra Steria Consulting Luxembourg



Lucas Colet
Lead Security Manager
Sopra Steria Consulting Luxembourg



Stéphane Badey
Partner
Arendt Regulatory & Consulting



Bénédicte d'Allard
Manager
Arendt Regulatory & Consulting

Agenda

- I. KYC and risk
 - Digitalization of KYC – an opportunity in a COVID 19 context
 - Feedbacks on current Risk and Security events
- II. Data protection of KYC data
 - GDPR applied to KYC data and process
 - Security measures
 - Risk and impact assessments
- III. Answers to our clients' top 10 questions
- IV. Our solutions – take aways

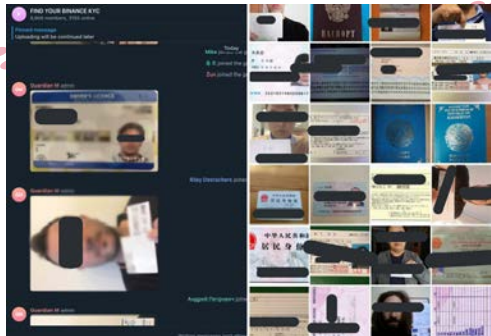
I. 1. Digitalization of KYC – an opportunity in a COVID 19 context

- Digitalization of KYC on the agenda of asset managers and service providers for years
- Range of solutions are available on the market from KYC utility to investors on-board in solutions
- Regulatory environment is evolving on the topic
 - Law of 20 March 2020 includes digital ID as a solution
 - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
 - Circular CSSF 20/740 Financial crime and AML/CFT implications during the COVID-19 pandemic
 - FATF, Guidance on Digital ID, 2020 (limited to physical Person)
- Great benefits but

I. 2. Current Risk and Security events: could it happen?

Binance KYC Data Leak – August 2019

The leak could affect up to 60,000 individual users who sent KYC information to the company in 2018 and 2019. They were stored at a third-party vendor.



- + Equifax (150 million people) – 2017
- + Russian MFIs (12 millions people) – 2020

Komisja Nadzoru Finansowego – Oct 2016 to Jan 2017

The website code of the Polish Financial Supervision Authority had been modified to cause visitors to download malicious JavaScript files. The malicious JavaScript led to the download of malware to the victim’s device. Visitors encompass several banks from all over the world, especially Poland, USA and Mexico. This attack is known as **waterhole attack**, like in nature, it is a place where several people are going to be fed. This attack has been attributed to **Lazarus Group**, a North Korean group very active in the financial world.

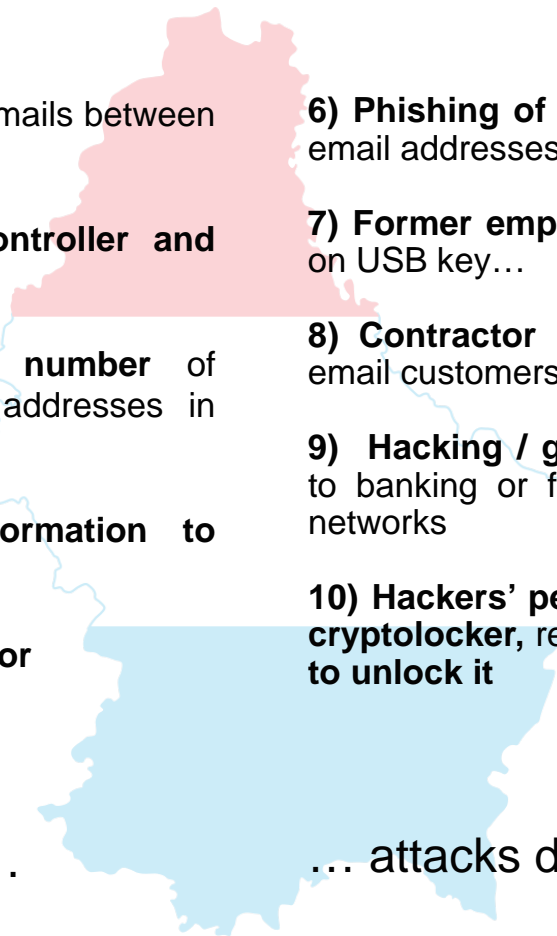
Three major Russian banks – June 2019

Personal Information of nearly 900,000 Banking Customers of three major Russian Banks leaked online. Customer data belonging to OTP Bank, Alfa Bank, and HCF Bank have been made publicly available on the internet. The data includes customer names, phone numbers, addresses, credit limit, passport details, and in some cases the place of work, year of birth, passport data, and account balance. Maybe disgruntled employees were at the source of this, or a hack has been perpetrated.

Digitex KYC Data Leak – March 2020

A former employee of Digitex, a digital asset derivatives trading platform, reportedly began leaking compromised know-your-customer (KYC) data via Telegram. The stolen data includes passport and drivers license images and other sensitive information which allegedly belongs to over 8,000 traders registered on Digitex.

I. 2. Current Risk and Security events: top 10 of (real) security events on KYC data in Luxembourg

- 
- 1) **Disclosure** of customers data via emails between several actors,
 - 2) Variant : the same **between controller and processor** (non encrypted data)
 - 3) Send an **email to a large number** of customers/investors with the email addresses in clear text
 - 4) **Error in sending (back) information to customers**
 - 5) Variant : the same but by a **processor**
 - 6) **Phishing of email boxes** followed by customers email addresses leak
 - 7) **Former employee** leaving with a list of investors on USB key...
 - 8) **Contractor** by the end of contract sending by email customers data...
 - 9) **Hacking / guessing of customers credentials** to banking or funds distribution platform on social networks
 - 10) **Hackers' penetration and lock out of data by cryptolocker**, resulting in unavailability, with **ransom to unlock it**

Mistake is often #1 source...

... attacks do also happen.

I. 2. Current Risk and Security events: understand risk origin and its motivation is key

Confidentiality

Data Leak

Hackers (*for money*)
Disgruntled (ex-)employee (*for revenge*)
Insider (*by mistake...*)

Data modification

Criminal / terrorist (*to make think they are safe*)
Insider (*by mistake...*)

Integrity

Availability

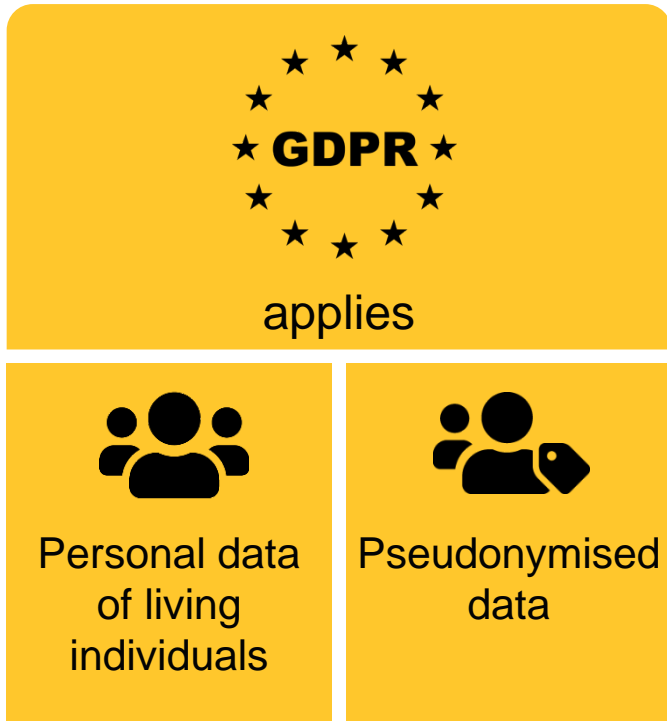
Access to your system

Hackers (*for money*)
Insider (*by mistake...*)

Data availability

Hackers (*for money*)
Disgruntled (ex-)employee (*for revenge*)
Insider (*by mistake...*)

II. 1. GDPR applied to KYC data



KYC data fall into GDPR scope of protection :
 Name (of NP), Account Number (of NP), Birth date, Profession, Shareholder ID Number (of NP), Tax Number (of NP), Private address, Account status (of NP), Private telephone / fax number, Bank details (of NP),...

Special categories of data : criminal records or relating to criminal convictions and offences, political and religious information.

Processing of personal data
 Any operation or set of operations performed upon personal data, whether or not by automatic means **collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.**

II. 1. Organizational protection principles

Ensure lawfulness, fairness and transparency

➤ Art (6)1c. Legal obligation

+

Minimize data

➤ Sticking to strict minimum collect

Limit purpose

➤ No re-use unless compatible

+

Ensure accuracy

➤ Regular review

Limit storage

➤ Deletion/ anonymisation when no longer necessary

+

Guarantee integrity and confidentiality

➤ Technical / organisational measures



In a digitalization context

II. 1. Mandatory documentation of processing activities gives a clear picture on KYC data/ process

- The Records of Processing activities (Art. 30) describes KYC data/ process in details, in particular:
 - Inventory of data types and data subject types
 - Inventory of applications used
 - Inventory of internal and external recipients allowing exhaustive identification of external interactions
 - Clarification of the company responsibilities (data controller vs data processor role) – impact on process in case of data breach or data subject requests.
 - Way of checking presence and appropriateness of data protection measures in place.
- The maintenance of relevant policies allows dissemination of protection rules, e.g. :
 - Data retention and deletion – avoid unlimited storage of data
 - Data subject requests – avoid blindly answering to unjustified requests
 - Data breach – quick and appropriate staff reactions may minimize damage.
- A Data processing agreement must be signed when relevant – protection measures in place at data processor must be ensured and reviewed on a regular basis.



- Increase protection of data (ex ante), and
- Support future investigations as relevant (ex post).

III. 2. Protection of AML/KYC data : Privacy and security measures 1/3

- **One of the 6 principles of the GDPR** requires that Data shall be ‘processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’
- In addition, **article 32 of the GDPR entitled ‘Security of processing’** requires that (...) ‘the controller and the processor implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing **confidentiality, integrity, availability** and resilience of processing systems and services;
 - (...)

III. 2. Protection of AML/KYC data : Privacy and security measures 2/3

- How to improve Personal Data Security (*and be secured AND compliant*)?
- ISO 27001 standard (Information Security) provides a framework
- Protect Personal Data's CIA : **C**onfidentiality, **I**ntegrity and **A**vailability using
 - Organisational Measures
 - Logical security measures
 - Physical security measures



What if a data processor is involved?

→ Carefully adapted to each organisation – risks and environments are different

III. 2. Protection of AML/KYC data : Privacy and security measures 3/3

■ Security helps business!



Being compliant (*to avoid fines*)



Keep reputation safe (*to avoid losing clients and then money*)



Traceability (*to know exactly what is done on your systems*)



Transform the processes (*to detect the incidents sooner, to avoid later higher costs*)

II. 3. Protection of AML/KYC data : Impact assessment of KYC data processing

- ‘ Where a type of processing (...) is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisaged processing operations on the protection of personal data.(...) in particular in the case of:

Is an Impact assessment of KYC data processing required ?

(a) a **systematic and extensive evaluation of personal aspects** (...) based on **automated processing, including profiling** (...)

(b) processing on a **large scale of “sensitive data” or of personal data relating to criminal convictions** (...)

(c) a **systematic monitoring of a publicly accessible area on a large scale.**
And **other processings listed by DP authorities**

Severity of harm on data subjects	Maximum	4	8	12	16
	Significant	3	6	9	12
	Limited	2	4	6	8
	Negligible	1	2	3	4
		Negligible	Limited	Significant	Maximum
		Likelihood			

II. 3. Protection of AML/KYC data : Impact assessment

What are
the main
risks ?

- Illegitimate access to data.
due to a data breach, a data
leakage...
- Unwanted data modification
- Data loss

Data protection by design,
Physical security,
Hardware security,
Fight against malware,
Traceability,
Manage risks,
Staff management,
Workstation management, Manage
Privacy policy,
Securing operations,
Data backup,
Partitioning,
Managing security incidents and
data breaches,
Encryption,
Archiving,
Securing paper documents ,
Maintenance, Logical access control,
Logging, Securing IT channels

What are the
main
measures to
be taken ?

arendt

Example
of a KYC-
AML tool

III. Your top ten questions

What is
....?

What are
the
main....?

**YOUR
MOVE !**

How
to... ?

What if....?

Is it
required
to...?

PLEASE ASK YOUR QUESTION IN THE Q&A SECTION

IV. Arendt – Sopra Steria GDPR compliance services

<p>Awareness</p>	<ul style="list-style-type: none"> ▪ Multi-client course ▪ Ad hoc client training
<p>Records of Processing activities</p>	<ul style="list-style-type: none"> ▪ Inventory of personal data processings and qualification based on GDPR principles ▪ Comprehensive gap analysis, or ▪ Synthetic Compliance scorecard
<p>Remediation support</p>	<ul style="list-style-type: none"> ▪ Policies/ procedures ▪ Documented instructions for processors ▪ Retention/ deletion of data ▪ Data Protection Impact Assessment (DPIA) ▪ Data Protection measures ▪ Information security assessment and improvement
<p>Data Protection Officer service</p>	<ul style="list-style-type: none"> ▪ Advice on DPO appointment ▪ External DPO mandate
<p>Other assistance</p>	<ul style="list-style-type: none"> ▪ Periodic board GDPR compliance dashboard ▪ Ad hoc advice

Visit our dedicated page ***Arendt Covid-19 Solutions*** and install the ***Arendt Insights App*** to find the most frequently asked questions and our answers



<http://bit.ly/ArendtCovid19Solutions>



<https://apps.apple.com/lu/app/arendt-insights/id1506580191>

Important Notice and Disclaimer : Whilst a best efforts approach has been taken to ensure the accuracy of the information provided in this presentation, as at the date thereof, this information is only designed to provide with summarised, and therefore non complete, information regarding the topics covered. As such, this presentation does not constitute legal advice, it does not substitute for the consultation with legal counsel required prior to any undertakings and it should not be understood as investment guidelines. If you would like to receive a legal advice on any of the issues raised in this presentation, please contact us.

Visit our dedicated page **Sopra Steria Covid-19** and check our very own **S@fe Office** solution to help manage all aspects of what a difficult return to normal operations might entail.



<https://bit.ly/SopraSteriaCovid-19>



<https://bit.ly/SafeOffice>

Important Notice and Disclaimer : Whilst a best efforts approach has been taken to ensure the accuracy of the information provided in this presentation, as at the date thereof, this information is only designed to provide with summarised, and therefore non complete, information regarding the topics covered. As such, this presentation does not constitute legal advice, it does not substitute for the consultation with legal counsel required prior to any undertakings and it should not be understood as investment guidelines. If you would like to receive a legal advice on any of the issues raised in this presentation, please contact us.

Contact us



Sylvie Dessolin
Senior Consultant
Sopra Steria
sylvie.dessolin@soprasteria.com



Lucas Colet
Lead Security Manager
Sopra Steria
lucas.colet@soprasteria.com



Stéphane Badey
Partner
Arendt Regulatory & Consulting
stephane.badey@arendt.com



Bénédicte d'Allard
Manager
Arendt Regulatory & Consulting
benedicte.dallard@arendt.com