

# Confidentiality and Security Requirements for the Global Translator



Monique Longton

monique@longtontranslation.com

[www.longtontranslation.com](http://www.longtontranslation.com)



*Listen (doo da do), do you want to  
know a secret? (doo da do)  
Do you promise not to tell? (doo da  
do)  
Whoa-oh-oh, closer (doo da do)  
Let me whisper in your ear (doo da  
do)...*



*The Beatles*



# Disclaimer

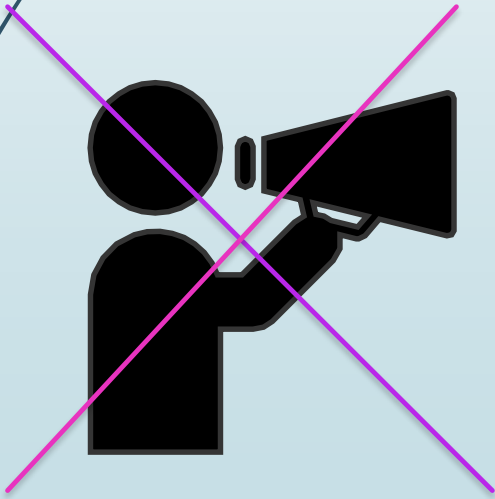
- The information provided on these slides does not, and is not intended to, constitute legal advice and is for general informational purposes only. The information presented here may not be current and is subject to change without notice. If you need legal advice, you should seek guidance from an attorney in the relevant jurisdiction.
- All materials contained on these slides are protected under copyright laws and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written authorization of Longton Linguistic Services.



# Session Outline

- 
- Session I: The legal framework
    - Introduction
    - Six good reasons to comply with our confidentiality and security requirements
    - Legal toolbox
  - Session II: Implementing our confidentiality and security requirements in our daily work and how to deal with reality
    - Creating a safe work environment
    - How to deal with reality?

# Introduction : Confidentiality/Privacy/Security?



## Confidentiality

Secrecy; the state of having the dissemination of certain information restricted

(Black's Law dictionary).

## Privacy

Privacy is the right to be let alone, or freedom from interference or intrusion.

Information privacy is the right to have some control over how your personal information is collected and used

(source: IAPP)

## Security

Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit.

(source: IAPP)

# Introduction

In the course of our daily activities, we translate a lot of information our clients do not want exposed:



Litigation

Attorney-client  
privilege

Principle of  
attorney-client  
confidentiality



Medical  
records



Government  
secrets

National  
defense  
secrets



Civil records

Resumes



Planned mergers

Prospectus (IPO?)



Patents

Trade secrets

# Introduction

Are you a website owner?

Other privacy and security requirements may apply to you.





# Session Outline

- Session I: The legal framework
  - Introduction
  - Six good reasons to comply with our confidentiality and security requirements
  - Legal toolbox
- Session II: Implementing our confidentiality and security requirements in our daily work and how to deal with reality
  - Creating a safe work environment
  - How to deal with reality?

# Six Good Reasons to Comply with Our Confidentiality and Security Requirements



Legal requirements



Codes of ethics



Contractual requirements



Cybercrime



Risks in the event of breach



Reputation/Success



# 1. Legal Requirements

## DUE DILIGENCE: KNOW THE LAW

### ► Privacy laws:

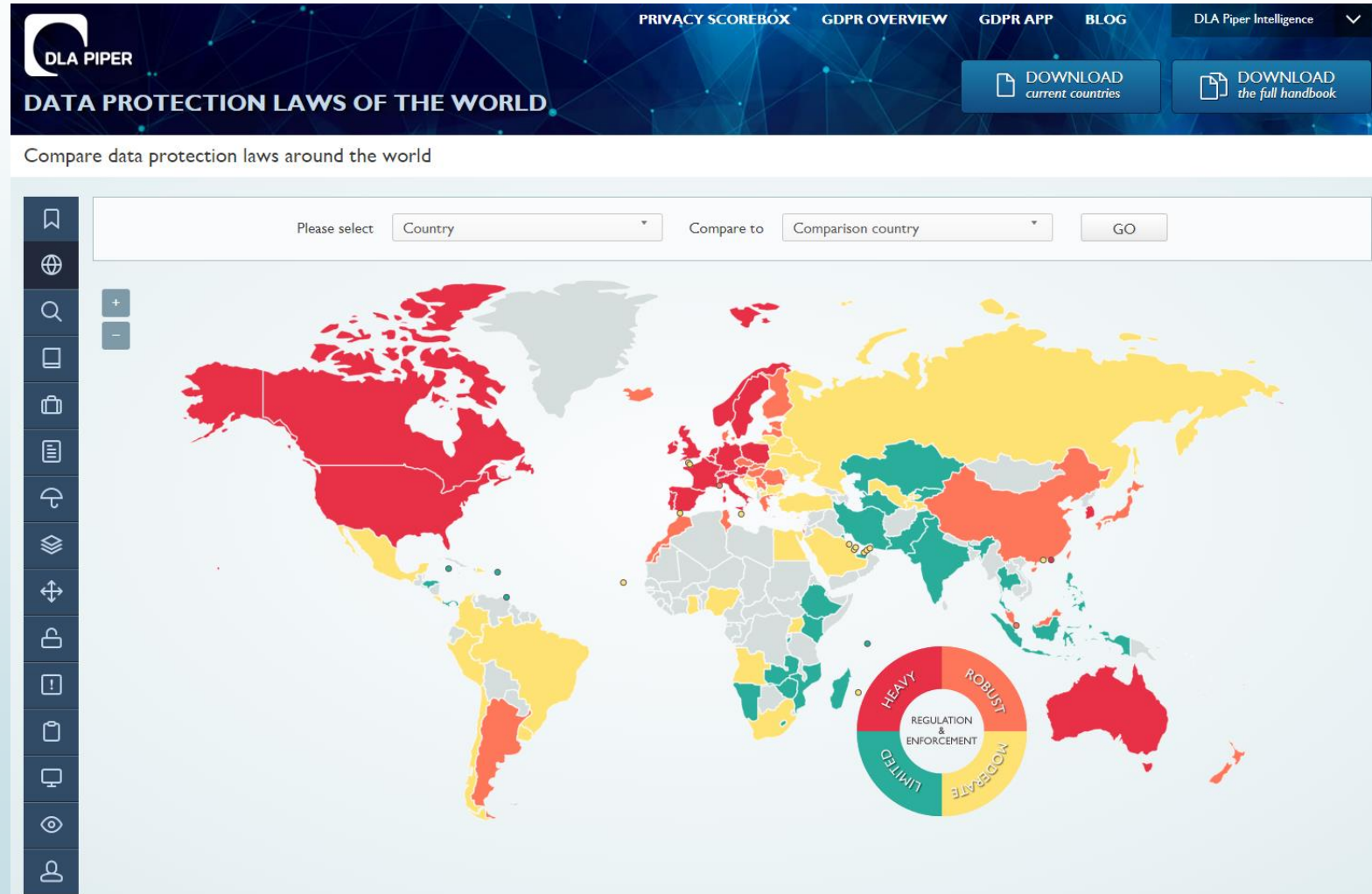
- General Data Protection Regulation (GDPR)
- National privacy laws around the world (e.g. EU Member States' national privacy laws, Canada: [Personal Information Protection and Electronic Documents Act](#) (PIPEDA))
- US State/EU member State privacy laws
- US privacy sectoral laws: HIPAA, COPPA, FATCA

### ► Specific sectoral laws:

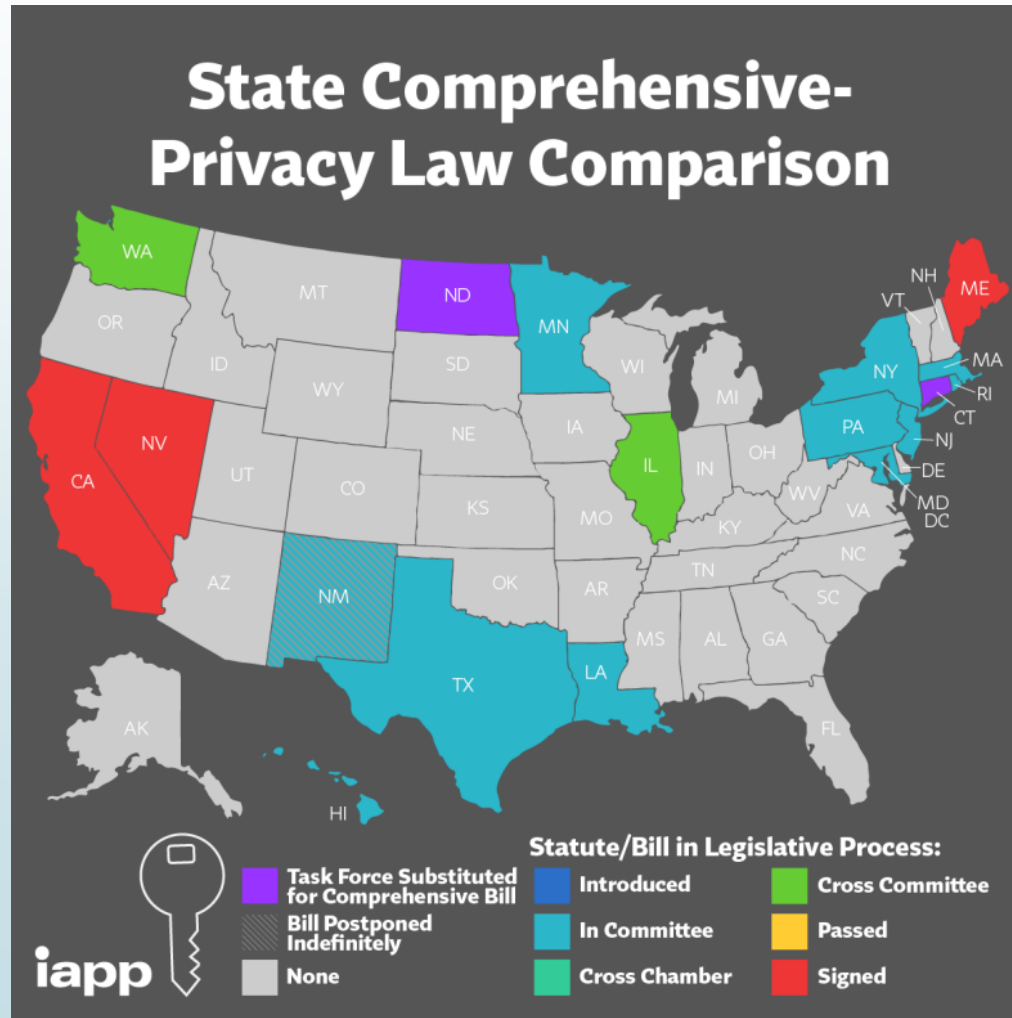
- Financial privacy laws (US: Bank Secrecy Act, Right to Financial Privacy Act, Gramm-Leach)Bliley Act, Fair Credit Reporting Act...)
- **US FTC:** Federal Trade Commission Act in the United States

# Privacy Laws Around the World

<https://www.dlapiperdataprotection.com/>



# US State Privacy Laws



- ➡ No federal law (yet?)
- ➡ Patches of state privacy laws
- ➡ Some federal sectoral laws

# The EU General Data Protection Regulation (GDPR): A Privacy Law with a Global Impact

Which GDPR hat are you wearing?



	When we do administration/ marketing and billing activities	When we translate
Who are we?	A Controller	A Processor or a Sub-Processor
Why?	We determine the purposes and means of the processing of personal data	We process the personal data on behalf of the controller
Main duties?	<ul style="list-style-type: none"><li>• Data protection by design and by default (GDPR, Art. 25)</li><li>• Allow the data subjects to exercise their rights (GDPR, Art. 12)</li><li>• Report any personal data breach to the Data Protection Authorities and the data subjects (GDPR, Art. 33)</li><li>• Comply with your transparency requirements (GDPR, Art. 12, 24)</li></ul>	<ul style="list-style-type: none"><li>• Process the data based on the data controller's instructions (GDPR, Art. 28)→Data Processing Agreement</li><li>• Protect the data subject's personal data (GDPR, Art. 28)</li><li>• Help the data controller meet their obligations (GDPR, Art. 28)</li><li>• Breach notification to controller</li></ul>



## The Brexit as of Oct. 22...

UK Parliament accepted Boris Johnson's withdrawal deal, but rejected his timetable

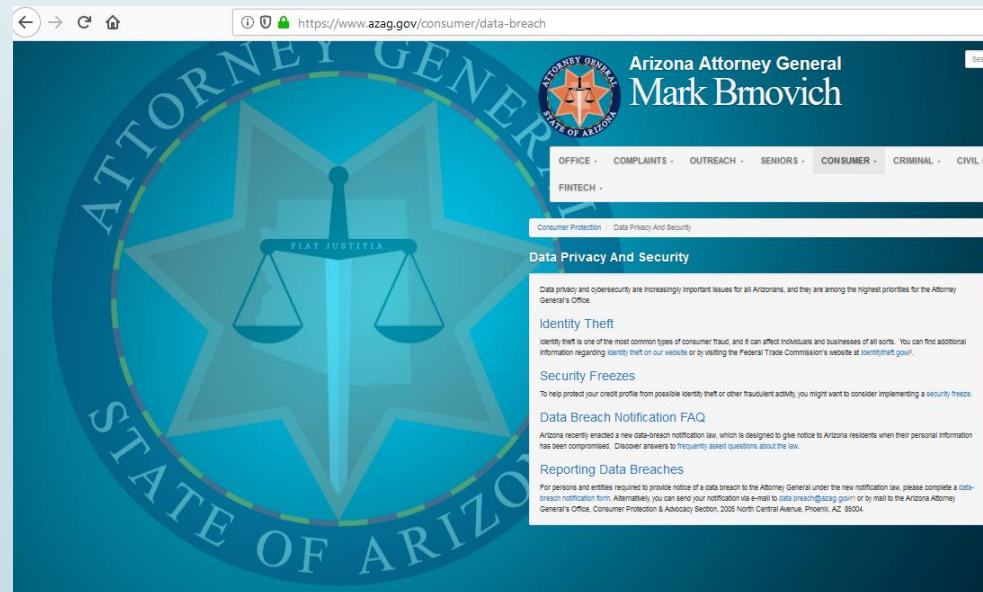
New Brexit extension requested to the EU

# Cybersecurity Laws in the US

- There is no US federal cybersecurity law. But, if you are a website operator, see Section 5: **Unfair or Deceptive Acts or Practices** of the **Federal Trade Commission Act**

<https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>

- A patchwork of laws and regulations pertaining to corporate cybersecurity practices





# Sectoral Privacy Laws: US Health Insurance Portability and Accountability Act (HIPAA)

- **Protected Health Information.** The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."12
- "Individually identifiable health information" is information, including demographic data, that relates to:
  - the individual's past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual,
  - and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

(source: HHS.gov –HIPAA Security Summary)



# HIPAA Requirements

- Privacy Rule on all Protected Health Information (PHI)
- Security Rule on electronic Protected Health Information
- Enforcement Rule (civil or criminal penalties, depends on severity of non-compliance)
- Breach Notification Rule
  - Unauthorized disclosure (system hacked, using unsecured Wi-Fi, device stolen or lost, sending email to wrong addresses)
  - Notify upstream



# UK – Official Secrets Act of 1989

## 8 Safeguarding of information.

- (1)Where a Crown servant or government contractor, by virtue of his position as such, has in his possession or under his control any document or other article which it would be an offence under any of the foregoing provisions of this Act for him to disclose without lawful authority he is guilty of an offence if—
  - (a)being a Crown servant, he retains the document or article contrary to his official duty; or
  - (b)being a government contractor, he fails to comply with an official direction for the return or disposal of the document or article,
  - or if he fails to take such care to prevent the unauthorized disclosure of the document or article as a person in his position may reasonably be expected to take.
- (2)It is a defence for a Crown servant charged with an offence under subsection (1)(a) above to prove that at the time of the alleged offence he believed that he was acting in accordance with his official duty and had no reasonable cause to believe otherwise.
- (3)In subsections (1) and (2) above references to a Crown servant include any person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force.
- (4)Where a person has in his possession or under his control any document or other article which it would be an offence under section 5 above for him to disclose without lawful authority, he is guilty of an offence if—
  - (a)he fails to comply with an official direction for its return or disposal; or
  - (b)where he obtained it from a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which that servant or contractor could reasonably expect that it would be so held, he fails to take such care to prevent its unauthorized disclosure as a person in his position may reasonably be expected to take.
- (5)Where a person has in his possession or under his control any document or other article which it would be an offence under section 6 above for him to disclose without lawful authority, he is guilty of an offence if he fails to comply with an official direction for its return or disposal.
- (6)A person is guilty of an offence if he discloses any official information, document or other article which can be used for the purpose of obtaining access to any information, document or other article protected against disclosure by the foregoing provisions of this Act and the circumstances in which it is disclosed are such that it would be reasonable to expect that it might be used for that purpose without authority.
- (7)For the purposes of subsection (6) above a person discloses information or a document or article which is official if—
  - (a)he has or has had it in his possession by virtue of his position as a Crown servant or government contractor; or
  - (b)he knows or has reasonable cause to believe that a Crown servant or government contractor has or has had it in his possession by virtue of his position as such.

# Your Legal Requirements – Conclusions



**Your homework: Know the law! Make a list of laws that apply to you**

**Three useful ATA presentations – but check for any changes since then**

- **ATA59: GDPR (contact Monique Longton)**
- **ATA55: HIPAA (contact Danielle Maxson)**
- **ATA58: Confidentiality in Translation (contact Emanuel Weisgras)**

## 2. Codes of Ethics

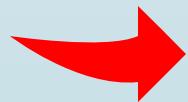
- ▶ ATA Code of Ethics, article 2:

"2. to hold in confidence any privileged and/or confidential information entrusted to us in the course of our work;"

- ▶ International Federation of Translators – Translator's Charter (source: [fit-ift.org.translators-charter](http://fit-ift.org/translators-charter)):

*10. The translator shall respect the legitimate interests of the user by treating as a professional secret any information which may come into his/her possession as a result of the translation entrusted to him/her.*

**Your homework: If you belong to a professional association, find out if their code of ethics applies to you.**



### 3. Our Contractual Obligations – Overview

Depending on the legal framework that applies, your client may ask you to sign agreements/you may have to set data retention periods

- Non-Disclosure Agreements
- GDPR:
  - Data Processing Agreements
  - Standard Contractual Clauses (which ones?)/Adequacy decisions
  - Cannot keep data forever
  - Data Processing Register (in most cases, optional but useful)
- HIPAA: Business Associate Contracts

**Any subcontractor agreement should be as comprehensive as a client agreement**  
**Otherwise, by definition, the subcontractor puts us at risk of breaching our contractual obligations**

# What Should Be in a Non-Disclosure Agreement?

- Identification of the parties
- Type of Agreement (Unilateral or Mutual)
- Relationship between the parties
- Definition of “Confidential Information”/Exclusions
- Data security requirements
- Non Disclosure of confidential client information **unless authorized or required by law**
- “Trickle down ” obligations (e.g. use of subcontractors)
- Boilerplate clauses

An NDA should not contain:



- Clauses that bind you to absolute secrecy
- Anything illegal or unethical
- Draconian penalty clauses



## When Information is No Longer/Not Confidential

- In certain cases, disclosure of confidential information may be required by law. Possible reasons may include:
  1. Evidence of criminality (past, ongoing, or future).
  2. Threat of imminent injury or death (i.e. suicidal ideations, death threats, etc.). This will often intersect with “evidence of criminality.”
  3. Required by judicial or quasi-judicial order.
- Any information already in the public domain/anything that enters the public domain (not because of the linguist)

# GDPR: Contractual Framework for the Translator as a Processor/Sub-Processor – Two Cases

- **Article 28** requires “a **contract** or other legal act under Union or Member State law”

1. **If you live inside the EEA**, only a data processing agreement

2. **If you live outside the EEA:**

1. Are you based in a country for which the European Commission took an adequacy decision ([https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en))?
2. If you're not, incorporate the “EU controller to non-EU or EEA processor Standard Contractual Clauses” in your data processing agreement ([https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en))
3. Right now: no Standard Contractual Clauses between EU processors and non-EU sub-processors



# GDPR: The Case of the US-Based Translator

- The European Commission took an adequacy decision for the United States: the **EU-UE Privacy Shield** (<https://www.privacyshield.gov>)
- **Privacy Shield Considerations:**
  - No need to sign Standard Contractual Clauses
  - You need to have a website (mandatory disclosures in your privacy notice)
  - You are subject to US federal law
  - Minimum fee of US\$ 500/year + average cost of US\$ 750 If you elect a US independent recourse mechanism
- **Standard Contractual Clauses:** You are subject to your client's EU jurisdiction





# What Should Be in a GDPR Data Processing Agreement ? (1/2)

- Purpose
- Description of the processing
- Duration of the agreement
- Processor's obligations with respect to the controller
  - Process the data for specific purposes
  - Follow controller's instructions
  - Guarantee confidentiality
  - Ensure people authorized to process the personal data are also bound by confidentiality requirements
  - Data by design and by default
  - Subcontracting



# What Should Be in a GDPR Data Processing Agreement ? (2/2)

- Data subjects' rights
- Exercise of data subjects' rights
- Notification of personal data breaches
- Assistance provided by the processor to the controller regarding compliance with its obligations
- Security measures
- Fate of data
- The data Protection Officer
- Records of categories or processing activities
- Documentation
- Controllers' obligations with respect to the processor



# What Should Be in a HIPAA Business Associate Agreement?

- Definitions
- Obligations and activities of Business Associate
- Permitted uses and disclosures by Business Associate
- Provisions for Covered Entity to inform Business Associate of privacy practices and restrictions
- Permissible requests by Covered Entity
- Term and termination
- Miscellaneous clauses



## 4. Cybercrime

Cybercrime hits the news daily...

- Marriott Hotel
- British Airways
- ... and probably your email almost daily

In its annual *Internet Crime Report*, the FBI reports the IC3 received 351,936 complaints in 2018—an average of more than 900 every day. The most frequently reported complaints were for non-payment/non-delivery scams, extortion, and personal data breaches.



## Ransomware sources

- ➡ Scam emails
- ➡ Infected websites
- ➡ Online ads
- ➡ Server vulnerabilities



## 5. Risks in the Event of Confidentiality Breach

- Civil liability
- Criminal liability
- Professional censure
- Loss of business and income
- GDPR: high administrative fines

## 6. Our Online Reputation

We're part of the supply chain



# Our Online Reputation

As privacy laws continue to develop, we need to care about our online image:

- Add a privacy notice to your website:
  - Must if doing business with EU/self-certified to EU-U.S. Privacy Shield
  - Check your national law requirements!!
- Add cookie policy
  - Can be part of your privacy notice

**If you state on your website that you protect your client's information, take real security measures to do so!**

**If not, it's considered as "unfair practices" in the US or "not transparent" practices in the EU!**





# Session Outline

- Session I: The legal framework
  - Introduction
  - Six good reasons to comply with our confidentiality and security requirements
  - Legal toolbox
- Session II: Implementing our confidentiality and security requirements in our daily work and how to deal with reality
  - Creating a safe work environment
  - How to deal with reality?

# Our Legal Document Toolbox

The following sources of information *must* be considered *only* as a starting point.

Please seek legal assistance to review your legal documents. This is NOT a recommendation or endorsement of any of these sources – simply a starting point.

## **1. Non-Disclosure Agreement Templates and Strategies for Drafting**

- <https://core.score.org/resources/non-disclosure-agreement-template>
- <https://eforms.com/nda/az/>
- [www.americanbar.org](http://www.americanbar.org)
- <https://techcontracts.com/sitefiles/wp-content/uploads/2016/05/MutualNDA.TechContractsHandbook-2016.05.25.docx>

## **2. HIPAA Business Associate Contracts**

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>

# Our Legal Document Toolbox

## 3. GDPR Data Processing Templates

- European Data Protection Authorities' websites:

[https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide\\_sous-traitant-cnif\\_en.pdf](https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnif_en.pdf)

- One **private sector** template:

[https://www.dlapiper.com/~media/files/insights/publications/2017/08/example\\_data\\_protection\\_addendum.doc](https://www.dlapiper.com/~media/files/insights/publications/2017/08/example_data_protection_addendum.doc)

## 4. European Commission Standard Contractual Clauses

[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)

## 5. Website Privacy Policy

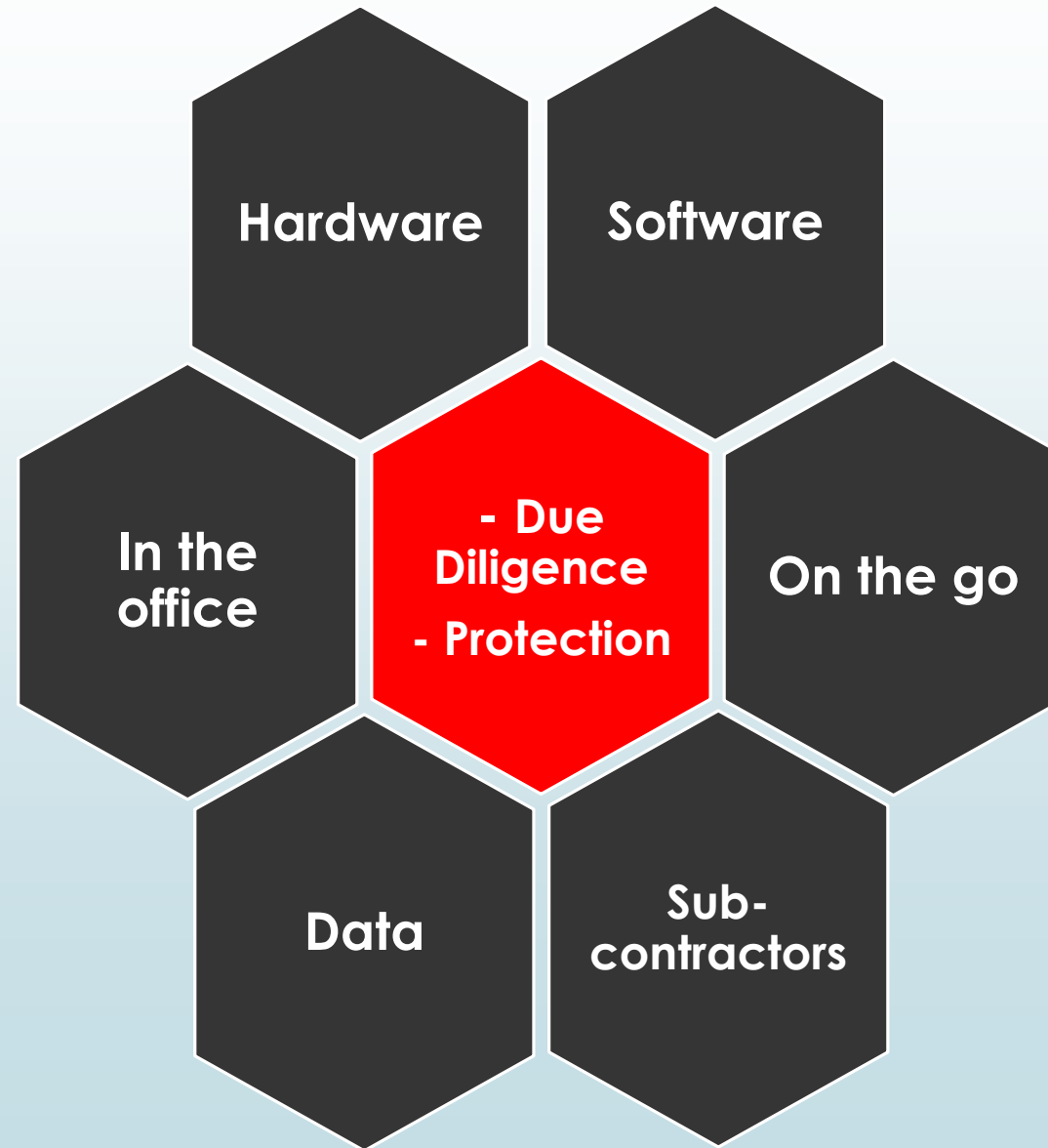
- [GDPR and EU Transparency Guidelines](#)
- [EU-U.S. Privacy Shield](#)

# Session Outline

- Session I: The legal framework
  - Introduction
  - Six good reasons to comply with our confidentiality and security requirements
  - Legal toolbox
- Session II: Implementing our confidentiality and security requirements in our daily work and how to deal with reality
  - Creating a safe work environment
  - How to deal with reality?



# Session 2 - Implementing Our Confidentiality And Security Requirements in Our Daily Work

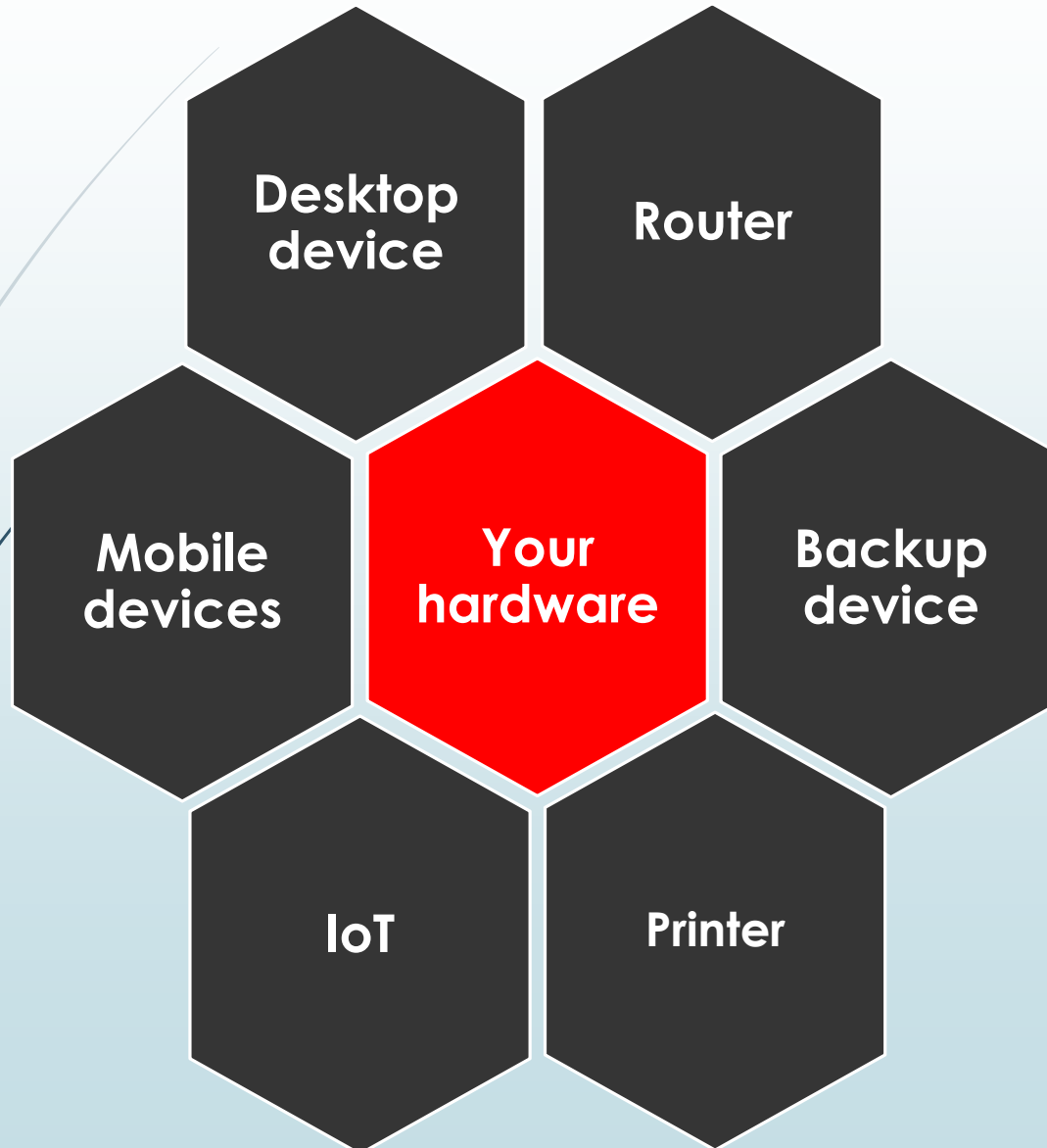


# Physical Security at Home or on the Go...



- Secure storage
- Limited physical access

# Your Hardware



- User/Password on your router
- Make sure your router offers WPA2 or WPA3 encryption
- Change mobile device settings to stop automatic connections to public Wi-Fi
- Apply security patches automatically
- Antivirus software at all times on all devices (mobile + desktop)
- Don't run your machine as an administrator

# 1. Due Diligence – Your Software



Before using any product:

- ❏ Read general terms and conditions  
Does the provider retain the right to use your data in exchange of "free" service?
- ❏ Consider your provider's business model (ad-based?)
- ❏ Geographical location of the provider's server
- ❏ Encryption in transit
- ❏ Encryption at rest on provider's server and/or password protection to access the shared file
- ❏ Search the news for any security incident
- ❏ Before you install an app to your business phone, restrict the privacy permissions




# 1. Due Diligence – Your Data



- Where is your data?
- What type of data do you have?
  - Public data
  - Internal data
  - Confidential data



# 1. Due Diligence – Your Subcontractors

- 
1. Are you allowed to subcontract your work?
    - a. Check your legal and contractual requirements

**Tip:** under GDPR, you need your client's express permission (GDPR, Art. 28.2)
    - b. If yes, do your due diligence work
  2. What measures does your subcontractor use to protect your client's data?

## 2. Protect Your Hardware, Your Software and Your Data (1/2)

- If you don't have an antivirus software, find one that fits your needs:
  - <https://www.pcmag.com/article2/0,2817,2372364,00.asp>
- Techniques to protect your data:
  - Data minimization
  - Data Retention Periods
  - Encryption
  - Anonymization
  - Pseudonymization
  - Archiving system

## 2. Protect Your Hardware, Your Software and Your Data (2/2)

### Golden Rules:

- **Never ever** click a hyperlink or open an attached file you do not trust within an email
- Make sure **all your devices are protected** against unauthorized access (phone, laptop, desktop, modem...)
  - Use **strong passwords**
  - Use **two-factor authorization** whenever possible
  - **Encrypt** any sensitive or personal data... anything that is important to you!
  - **Don't keep your passwords on your device**
- Set your devices to apply **security patches automatically**
- Use an **antivirus** software at all times on all devices
- **Only keep the data you absolutely need on your working computer**
- **Never ever ever...** send sensitive information over email, text message or any unsecure platform (check <https://signal.org/>)
- **Don't use the Wi-Fi in public places without a VPN**
- **Back up your data:**
  - Cloud (check [www.carbonite.com](http://www.carbonite.com))
  - Local: use at least two separate devices
- **Keep up with the security news**

# Password Management

- Time needed to crack a password through a brute force attack
  - Password123: instantly
  - Spaghetti95!: 48 hours
  - Spaghetti!95: 24 hours
  - A&d8J+1!: 2.5 hours
  - I don't like pineapple on my pizza!: more than one year

Source: Australian Government, Australian Signals Directorate, Small Business Cyber Security Guide

- Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.
- Minimum requirements (CNIL): minimum 12 characters, includes upper-case letters, lower-case letters, numbers, and special characters
- Never reuse passwords and don't share them on the phone, in texts, or by email.
- Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.



# Data Retention

- Anonymize your TMs if you can
- Only keep your data for the required time
  - Implement system of data layers:
    - Archive data which is no longer used on a daily basis, but must be kept

# Examples of Tools

Purpose	Name	Source
Antivirus		<a href="https://www.pcmag.com/article2/0,2817,2372364,00.asp">https://www.pcmag.com/article2/0,2817,2372364,00.asp</a>
Encryption	7-zip	<a href="https://www.7-zip.org/">https://www.7-zip.org/</a>
	VeraCrypt	<a href="https://www.veracrypt.fr/en/Home.html">https://www.veracrypt.fr/en/Home.html</a>
	OpenPGP	<a href="https://www.openpgp.org/">https://www.openpgp.org/</a>
	Bitlocker	<a href="https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption">https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption</a>
Multipurpose	Office365 (E3 or E5 subscription or Azure subscription)	<a href="https://products.office.com/en-us/compare-all-microsoft-office-products-b?&amp;t41437&amp;activetab=tab:primaryr1">https://products.office.com/en-us/compare-all-microsoft-office-products-b?&amp;t41437&amp;activetab=tab:primaryr1</a>
Password Manager	LastPass	<a href="https://www.lastpass.com/get-premium?&amp;gclid=EAlalQobChMloPzMnemy5QlVNB-tBh1w_AyiEAAYASAAEgKPM_D_BwE">https://www.lastpass.com/get-premium?&amp;gclid=EAlalQobChMloPzMnemy5QlVNB-tBh1w_AyiEAAYASAAEgKPM_D_BwE</a>
	KeePass	<a href="https://keepass.info/">https://keepass.info/</a>
Email	Choose an email provider that offers encryption capability or e.g. integrates with e.g. OpenPGP	
Instant Messaging	Signal/Telegram	<a href="https://signal.org/">https://signal.org/</a> <a href="https://telegram.org/">https://telegram.org/</a>
Backup solutions	Carbonite or 2 separate offline devices	<a href="https://www.carbonite.com/">https://www.carbonite.com/</a>



# Session Outline

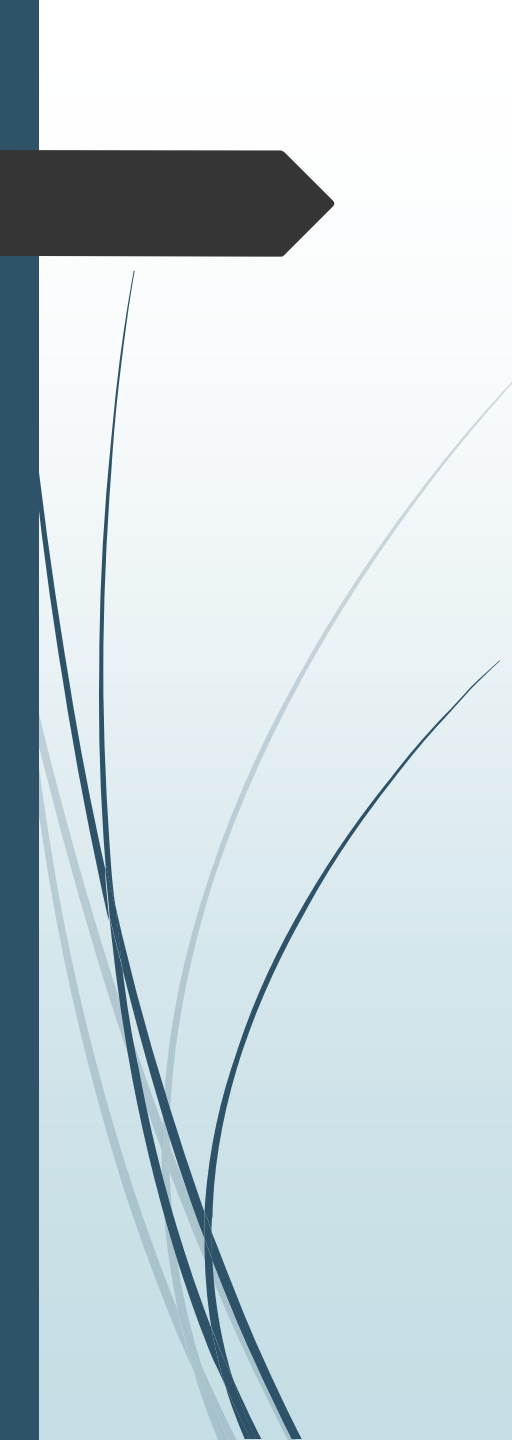
- Session I: The legal framework
    - Introduction
    - Six good reasons to comply with our confidentiality and security requirements
    - Legal toolbox
  - Session II: Implementing our confidentiality and security requirements in our daily work and how to deal with reality
    - Creating a safe work environment
    - How to deal with reality?
- 



# How to Deal with Reality?

## ➤ **KNOW THE LAW**

- Clients may not know their legal requirements and/or may choose to ignore it
  - "Not me" syndrome...
- Be gentle with your clients, but keep trying, and **DOCUMENT everything** you try and keep your proof in a safe place
  - 1. Read your contracts and understand them
  - 2. Ask for contractual changes
  - 2. Propose a contractual template if your client does not have one
  - 3. Always propose alternatives to exchange information securely
- As per GDPR, the burden will be on your client, but it is also your duty to remind your client of their obligation



*“Help, I need somebody  
Help, not just anybody  
Help, you know I need someone, help”*

The Beatles

Questions, anyone?