

52th Congress of the European Bars Federation "Right to privacy in a digital age"

## Small law firms and full understanding and application of data protection rules: are they really irreconcilable?

## Frequent misunderstandings and risk underestimations about security of clients' data

Warszawa September, Thursday 20th 2018

Avvocato Francesco Tregnaghi Verona Bar Council - Italy



### DIRECTIVE 95/46/EC preamble (old "privacy" directive)

Article 1 started with..." In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

#### **GDPR preamble** REGULATION (EU) 2016/679

#### Art 1

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

#### **Different eras**

- In 1995 the digital revolution was just starting. The digital data treatment, elaboration and net diffusion has started only for very big public institutions and companies.
- In 2016 even the smallest firm or professional uses a computer connected to internet, and carries a smartphone potentially full of data

#### From "privacy" to "data protection"

Just the introduction of the two ruling acts shows a <u>different point of view</u> of the European legislation, reflecting the evolution of the times.

From "privacy" (I can't sell or give away the data I manage) to "data protection": More than that, I have to take positive action also to protect those data from all the risks they are exposed to in actual environments

#### Article 24 Responsibility of the controller

CHAPTER IV Controller and processor - Section 1 General obligations - Article 24 Responsibility of the controller

"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation..." (accountability)

#### **Security breach notification**

- According to Article 33, a law practice acting as data controller must notify personal data breaches to the supervisory authority without undue delay, and in any event not later than 72 hours after having become aware of such a breach.
- In certain high risk cases, the law practice is also required to notify its clients directly (Article 34), though there are special exemptions.

#### A general view on data protection

Protecting data you manage, apart not willingly giving them away, include:

- Make sure data is not stolen (security, security and even more security)
- Make sure data is not accidentally lost (redundant backup, with increased concern about security)

#### **Small law firms and data protection**

## Every single-lawyer firm (remember: no mandatory DPO!) must <u>understand what data</u> <u>protection may be</u>

But, most of all What is not!

#### **1 - Unprotected Smartphones**

#### What do I meed protected access or data encryption for? I do not have clients' data on it!

**Really?** 

Do you have your work emails on it?

Do you have the same cloud storage access than you have in your office computer?

What? Well, maybe. I don't have a clue.

Yes!

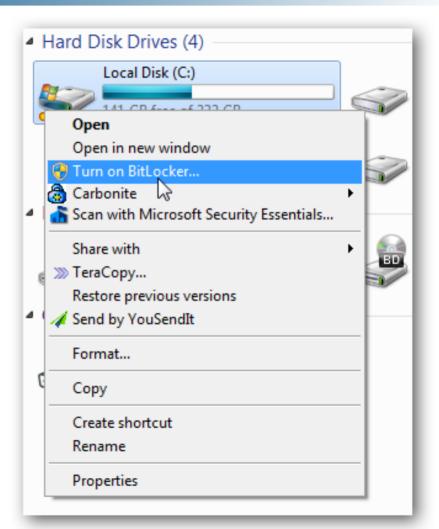


# 2 - Unencrypted portable backup devices

#### Hey, my work files and data are backupped! And, for redundancy and security, I bring them home, too!

Many Colleagues do this (and for a good reason) but if the portable device is not encrypted, this a HUGE risk for data protection!

Very few knows that is very easy to protect those devices.

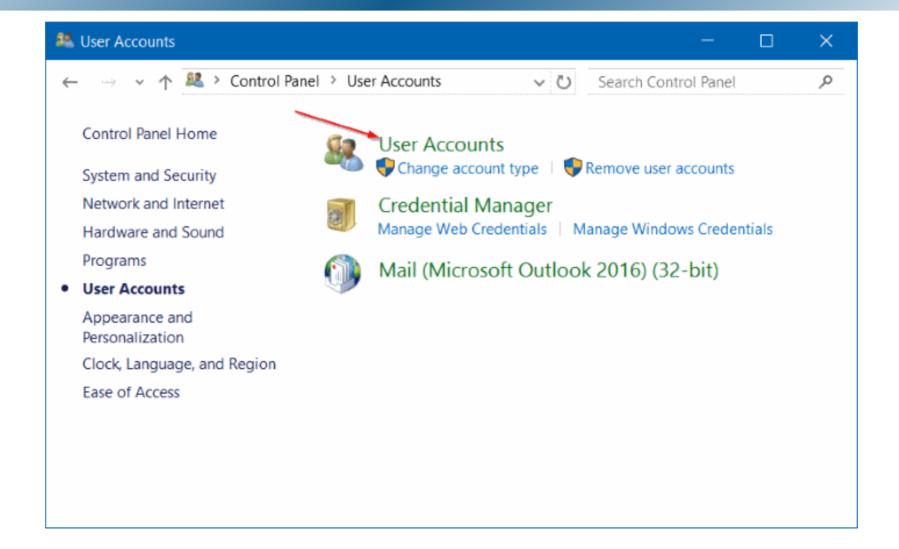


#### **Unlocked personal computers**

A frequent mistake is not to **protect the user account with a password**, or not setting the **screensaver** to ask it again whenever the screen resumes after a pause.

This helps not only unauthorized access from people in front of the physical device, but, most of all, makes **accessing the computer from the network** much, much easier.

#### Managing accounts is easy



#### **Unencrypted sensitive data**

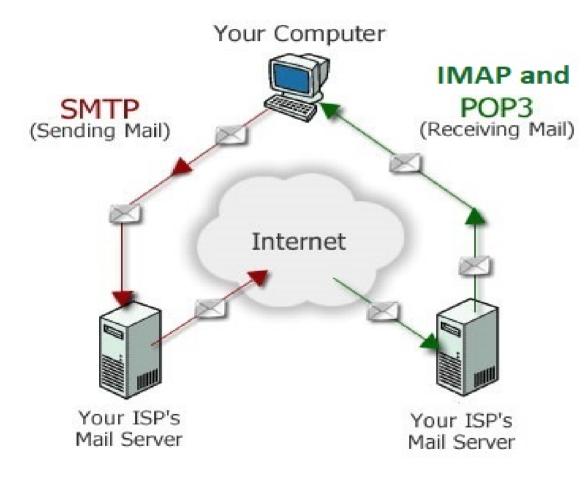
Protecting the user access means nothing is someone has in his hands the physical disk (e.g. on a stolen laptop). Accessing it from another O.S. is very easy, and all data are readable.

Most modern operating systems (in Windows since XP, in the highly recommendable "pro" version) have **built-in full disk encryption,** which will encrypt the entire contents of the drive. The data is decrypted when the user accesses the device. Unfortunately, it may not be enabled by default, requiring action to be activated

### Activating encryption on single folders

Private Properties ×	DATAPART1 (D:) > Documents > ClientsData	
<ul> <li>Choose the settings you want for this folder.</li> <li>When you click OK or Apply on the Properties dialog, you rasked if you want the changes to affect all subfolders and as well.</li> <li>Archive and Index attributes</li> <li>Folder is ready for archiving</li> <li>Allow files in this folder to have contents indexed in addition to the properties of the prope</li></ul>	d	
Compress or Encrypt attributes Compress contents to save disk space Encrypt contents to secure data Detai		text document.txt
OK Car		

#### **E-Mail servers unsecure access**



### POP3, SMTP, IMAP are UNSECURE protocols.

Any good hacker, from anywhere, could read the emails in the same moment we download or upload our messages from/to mail servers. And read the passwords for future accesses, too.

The equivalent but encrypted **POP3s, SMTPs, IMAPs** (where "s" stands for secure) must be used instead.

They use one of the secure encrypted protocols

### **Too simple passwords**

 $\leftarrow$ 

Most commonly used Pws according to Password manager "Keeper" Rank 2016

- 1 123456
- 2 123456789
- 3 qwerty
- 4 12345678
- 5 111111
- 6 1234567890
- 7 1234567
- 8 password
- 9 123123
- 10 987654321



....

Your password would be cracked



#### **Shared LAN resources**

Many small law firms share the offices with colleagues or other professionals, sharing printers, internet access and LAN resources.

If the resources sharing isn't controlled and set with the needed security permissions, a lot of data may result accessible to people that should not read/copy/ modify them.

Any shared resource should be protected with correct permission policies

## Managing folder permissions

You ci	Security Customize an share this folder with other users on your k. To enable sharing for this folder, click Share this		
O Do not sha			
<ul> <li>Share this</li> </ul>	folder		
Share name:	My Folder		
Comment:			
User limit:	O Maximum allowed		
	Allow this number of users: 10		
	ions for users who access this Permissions Permissions		
To configure s Caching.	ettings for offline access, click Caching		
with other comp	all is configured to allow this folder to be shared outers on the network. lows Firewall settings		

Permissions for Program Files	×			
Security				
Object name: C:\Program Files				
Group or user names:				
& CREATOR OWNER				
SYSTEM 8				
Administrators (Veradi-Home)	Administrators)			
& Users (Veradi-Home\Users)				
88 TrustedInstaller				
	Add Remove			
Permissions for CREATOR OWNER	Allow Deny			
Full control				
Modify				
Read & execute				
List folder contents				
Read				
Learn about access control and permissions				
ОК	Cancel Apply			

#### Wifi network access

WiFi access to LANs containing data should be, if necessary

- Protected by the most efficient transmission protocol
- Access should be limited to specified devices (using their MAC addresses)
- Turned off when not necessary (many WiFi routers have automatic timed turn-off and on)

## WiFi settings

ኛ WiFi Auto-Off	
TURN WIFI ON	
when device gets unlocked	
everyday at 8:05	
every 2 hour(s)	
TURN WIFI OFF WHEN	
screen is off for at least 10 min	
not connected to any network for at least 1 min	•
everyday at 22:00	

 $\Box$ 

t)

<b>D-Lini</b>	_						
DIR-825	SETUP	ADVANCED	TOOLS	STATUS	SUPP		
VIRTUAL SERVER	MAC ADDRESS FIL	TER			Helpful Hint		
PORT FORWARDING	The MAC (Media Access	Controller) Address filter	option is used to contro	ol network access	Create a list o addresses tha		
APPLICATION RULES		ess of the network adapt			either like to a access to you		
QOS ENGINE	network/Internet acces	e network adapter. This fo s.	eature can be configure	d to ALLOW OF DENY	Computers th		
NETWORK FILTER	1()	ave Settings			obtained an If		
ACCESS CONTROL	Save Settings Don't S	ave setungs			server will be Client List, Sel		
WEBSITE FILTER	24 MAC FILTER	ING RULES			from the drop menu, then di		
INBOUND FILTER	Configure MAC Filtering	below:			to add that de		
ROUTING	Turn MAC Filtering OFF						
ADVANCED WIRELESS	MAC Address	DHCP Clier	nt List		Click the Clea remove the M from the MAC		
WI-FI PROTECTED SETUP	00:00:00:00:00:00	4 << Computer N	Name 🔻	Clear	More		
ADVANCED NETWORK	00:00:00:00:00:00	< Computer N	Name 🔻	Clear			
GUEST ZONE	00:00:00:00:00:00	< Computer N	Name 🔻	Clear			
IPv6	00:00:00:00:00	< Computer N	Name 🔻	Clear			
	00:00:00:00:00	<	Name 🔻	Clear			
	00:00:00:00:00	<	Name 🔻	Clear			
	00:00:00:00:00	< Computer N	Name 🔻	Clear			
	00:00:00:00:00	< Computer N	Name 🔻	Clear			
	[]		1				

#### **Multi-function printers/scanners**

Modern network scanners have built-in hard-disks to store scanned documents, that will be later picked by the interested lawyer. Those files are not erased automatically. This is unacceptable in shared LANs. But, whorst...



In a recent case, a firm that bought a second-hand machine from a leasing company found a full hard-disk of PDF documents, clearly and easily identified as documents scanned by a Milan medium-sized law firm!



#### **Cloud Storage**



Cloud storage is fantastic. We can work from everywhere and the backup is assured by well organized third-parties. There are even excellent ones for free.

- It must be of course protected with a strong password.
- It should be hosted in EU since the <u>US Patriot Act</u> still clashes with EU data protection environment, and to store data in a server subject to it would be a violation of the EU regulations

#### Cryptolocker 2.0

#### Your personal files are encrypted

Info



Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files

and try to open them.

Encryption was produced using **unique** public key <mark>RSA-4096</mark> generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click proceed to payment to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.



#### **Troyan / Virus threats**

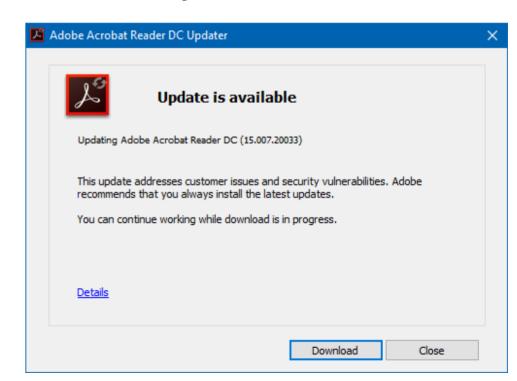
Malware may attempt both privacy and security of "our" data.

- Some are designed to <u>secretly steal data and passwords</u>.
- Some others (<u>ransomware</u>) do not steal your data, but encrypt all of them (and all the real time backups are affected, of course), and promise the decryption key only by paying a ransom. Even if you pay, sometimes all data are lost forever
  - An up-to-date anti-malware/antivirus is vital, as well as backup policies that consider the risk of all the connected resources to be compromised at once.

#### Software updates

 All the software we use, starting from the device OS and with special regards with software with internet access, should be upgraded to the last release, to avoid security leaks.





#### What to do

- We need not to sleep over our habits, but consider threats are always changing, as the environment we are connected to improves.
- We have to <u>analyze</u> our "digital environment" to understand the risks
- We have then to <u>plan</u> accordingly, to erase or reduce those risks
- …and to comply GDPR!

# How can I understand the real risk in my environment?

DPIA (Data protection impact assessment, art 35) even when non-mandatory may be a very useful instrument to identify risks.

The French authority (www.cnil.fr) developed an open-source and multi-language software that may be a very useful guided instrument to analyze our data environment and identify risks

### Should a lawyer become an IT expert?

- No, of course. But a certain degree of IT skill is required. If lacking, a civil or even <u>deontological</u> <u>responsibility</u> may occur (CCBE Guidance 2016)
- Even though most of the actions to take to avoid the exposed risks are not so difficult, a lawyer may use help from a technician BUT
- <u>he personally must know the risks</u> and make sure all of them are considered and minimized, AND
- must <u>learn and follow the good practices</u> in data protection in every-day's life



Francesco Tregnaghi Avvocato – Verona, Italy www.tregnaghi.it @Effetiverona

Credits:

Thanks to Francesco Paolo Micozzi, of the Cagliari Bar