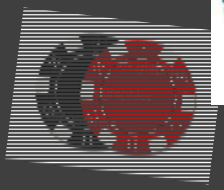
Meet the Cast of Characters…

Little Red Riding Client

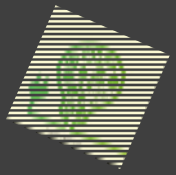
- A US-Based Corporation
- Or a multinational
- Doing business with individuals who reside in the EU

Various sizes and industries










Grandma

- The Data Protection Directive (95/46/EC)
- Existing EU data protection law which applies mostly within the borders of the European Economic Area

The Big Bad GDPR

- EU General Data Protection Legislation (GDPR)
- Overhauls EU data protection legislation
- One law directly applies to all 28 states
- Effective date: May 25, 2018

That was then…

- Little Red Riding Client has been doing business with EU clients and end users, without any regard to EU data protection laws.
- EU Data protection laws did not apply to it

This is now….

- GDPR is a game changer
- It applies to US companies even if they do not have a physical presence in the EU
- It raises the stakes
- It cannot be ignored

Extensive extraterritorial jurisdiction

GDPR applies to US companies if they

- set out to provide services to individuals residing in the EU

and those services

- involve processing identifiable personal information

OR

- Track / monitor EU individuals (cookies)

Big Fines

- Fines are the larger of:
  - 20 Million EUR OR **4% of worldwide revenue**
  - 10 Million EUR OR **2% of worldwide revenue**
- Calculated based on group of companies

Meet the Protagonist…

Legal and Compliance GDPR Team

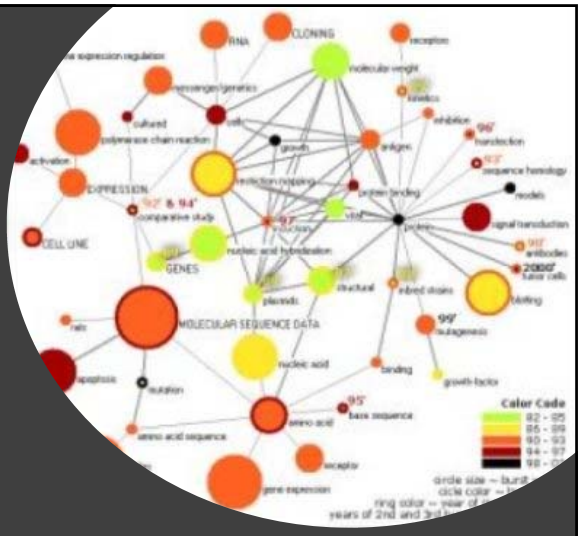
- Provide pragmatic, risk mitigation strategies for GDPR compliance.
- Complete compliance programs or specific issues / projects.

Daunting Task List for Compliance

- US Companies are considerably behind their EU counterparts.
- Do not have policies, procedures and necessary for GDPR compliance.
- Large changes may be required in operations, products, and paperwork.

Where in the world is my data?

- What data do I collect?
- Why do I collect it? Do I need it?
- Do I have permission?
- What do I use it for?
- Who do it share it with?
- What do they do with it?
- How long do I keep it for?



What is my legal basis?

- It's just consent, right?
- Contract
- Compliance with a legal obligation
- Protection of vital interests
- Performance of a task in the public interest
- Legitimate interest

What should my privacy notice say?

- It is NOT the website privacy notice law
- It's a NOTICE not a policy
- It DOES cover cookies
- But also offline collection
- Other laws cover cookies too
- Do I collect personal data?
- Where do I get it?
- What is my legal basis?
- What do I use it for?

What <u>else</u> should my privacy notice say?

- Who do it share it with?
- What do they do with it?
- How long do I keep it for?
- Am I sending it overseas?
- What are people's rights regarding the data?
- Where can people complain if I messed up?

Can I take "yes" for an answer?

- Consent under GDPR is complicated
- Not implied, no pre-ticked boxes.
    - Freely given
    - Specific
    - Informed
    - Unambiguous

Service Providers

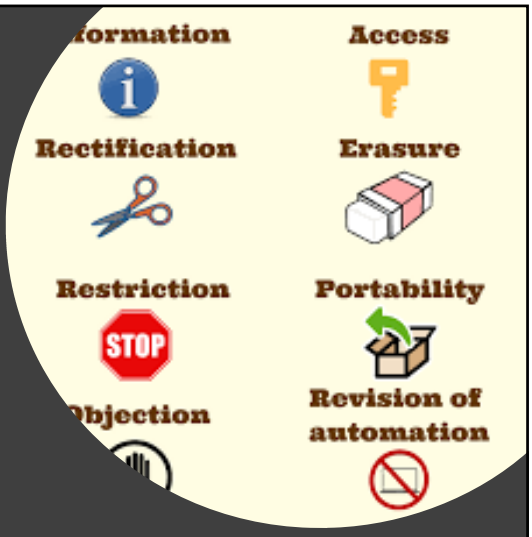
- Who handles personal data for me?
- Can they be trusted? What about their personnel?
- What does my agreement with them say?
  - What can they do with my data?
  - Can they outsource?
  - Can they transfer data overseas?
  - Can they help me with people's requests?
  - What if they get hacked?

Last call for data transfer

- Is the data leaving the EU?
- Is it going to the US?
- Do I have something to make this transfer "kosher"?
  - Model clauses?
  - Binding corporate rules
  - EU US Privacy Shield certification

What do I do about people's requests?

- Do I need to give them access to their data?
- Do I need to let them correct the data?
- Can then tell me to stop certain uses of their data?
- Do I need to delete their data?
- Do I need to give them a copy of their data?
- What can they do if I messed up?



What if I got hacked?

- Notify the data protection authority within 72 hrs unless there is no risk to the rights of individuals
- Notify individuals without undue delay if there is a high risk to the rights

DPIA: What if I <u>think</u> my data processing is risky?

- What is the processing?
- Is it necessary?
- Is it proportional to the need?
- What risks does it pose to people?
- What can be done to mitigate the risks?

DPO: What if I <u>know</u> my data processing is risky?

- regular and systematic monitoring of data subjects on a large scale OR
- processing on a large scale of special categories of data

Do I engage in profiling?

- Do I use automated processing of personal data to evaluate personal aspects like work performance, economic situation, health?
- Am I making decisions decision based solely on automated processing, including profiling, which produce legal effects concerning the individual or similarly significantly affects the individual?

Odia Kagan

Partner, Chair of GDPR Compliance and International Privacy

Fox Rothschild LLP

okagan@foxrothschild.com

215-444-7317