Eve of the GDPR

Take Stock & Carry On

Sarah Clarke, CIPP/E
Privacy and Security GRC Specialist
Owner Infospectives Ltd (@TrialbyTruth)

Image credit: 123rf Stock Photo:vkovalcik

DUCK and COVER

Image credit: 123rf Stock Photo: volkoff

Check the taps

Image credit: 123rf Stock Photo: Leonid Ikan

Check the drains

Image Copyright: 123rf: Igor Plotnikov

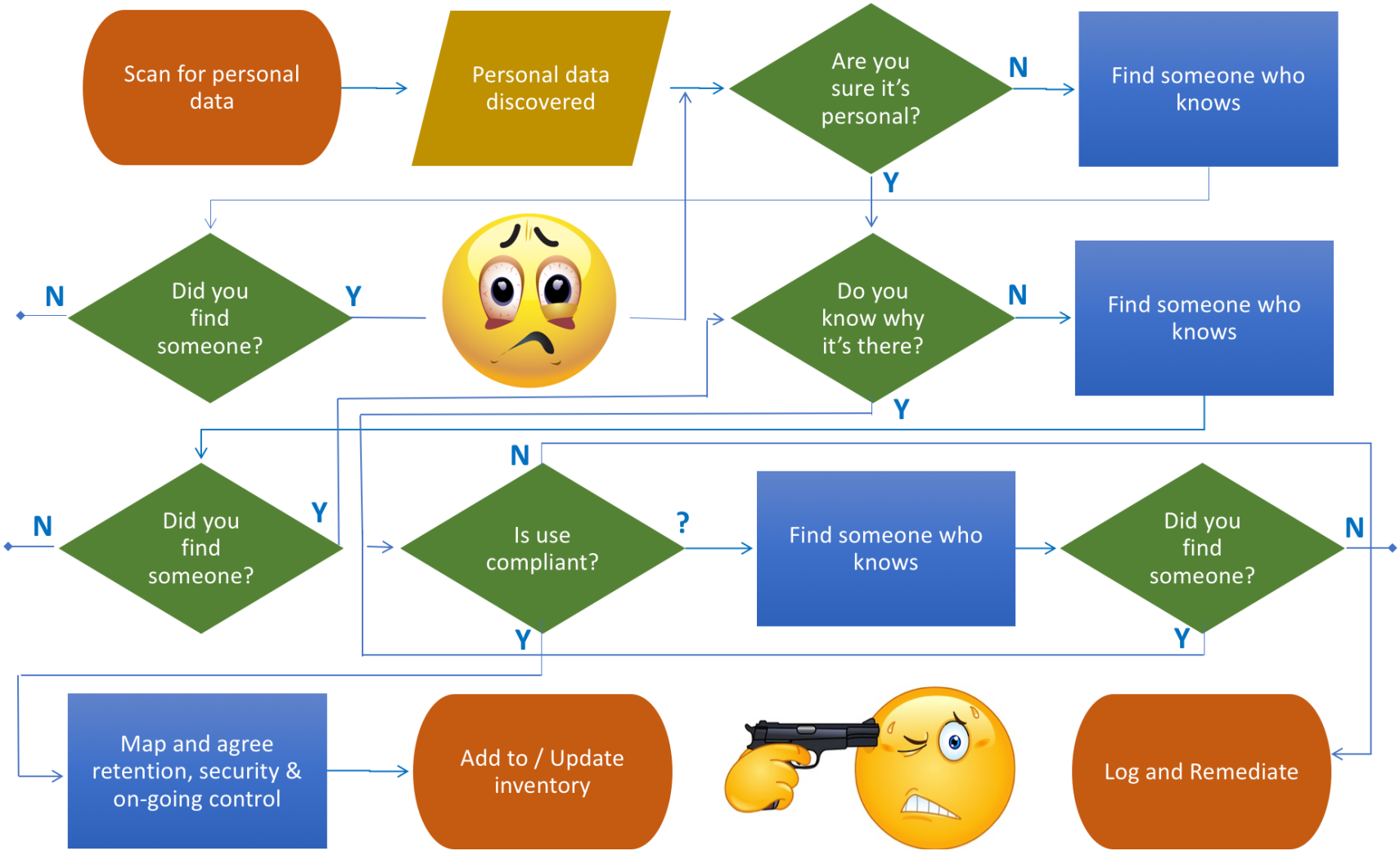
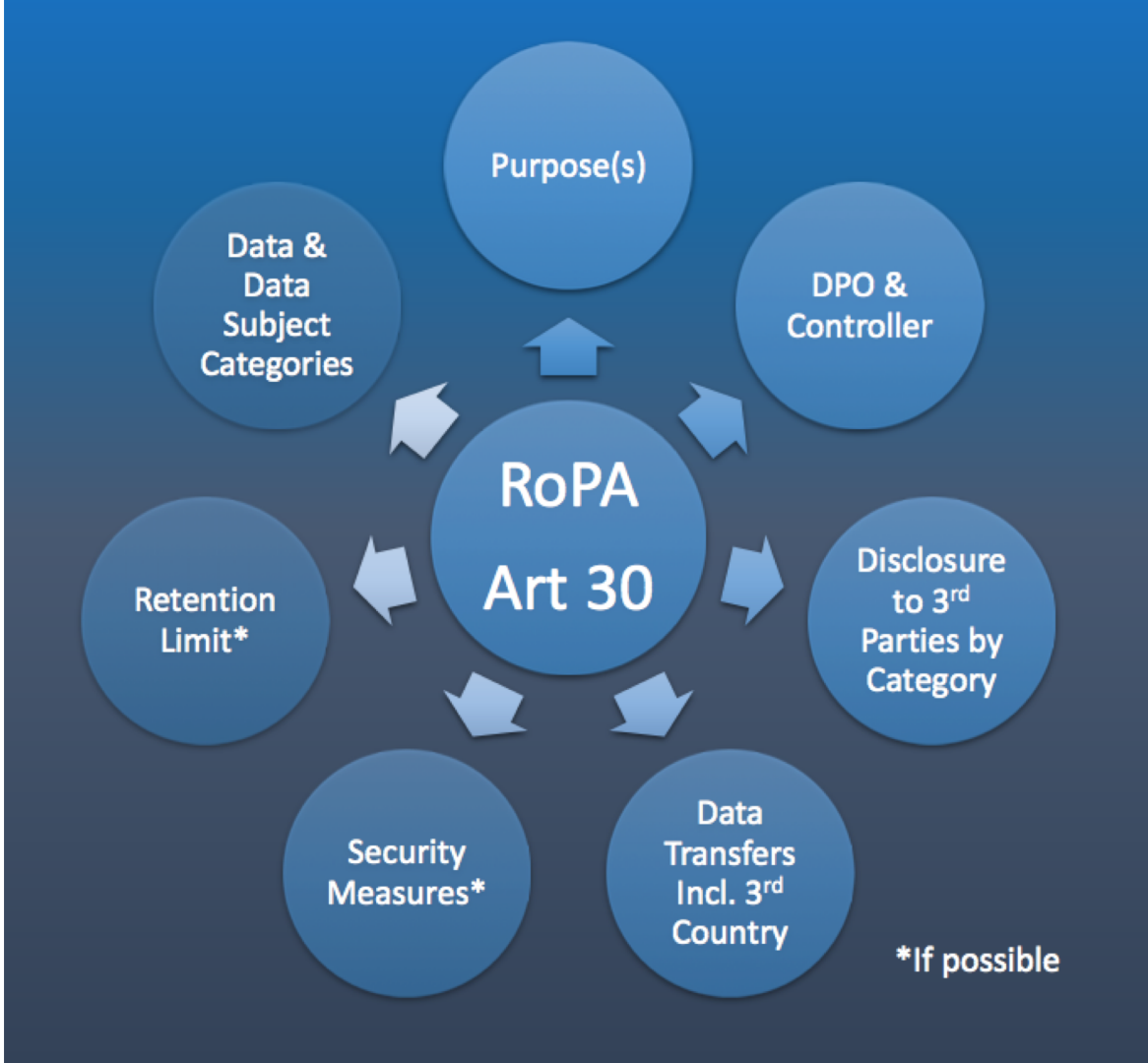
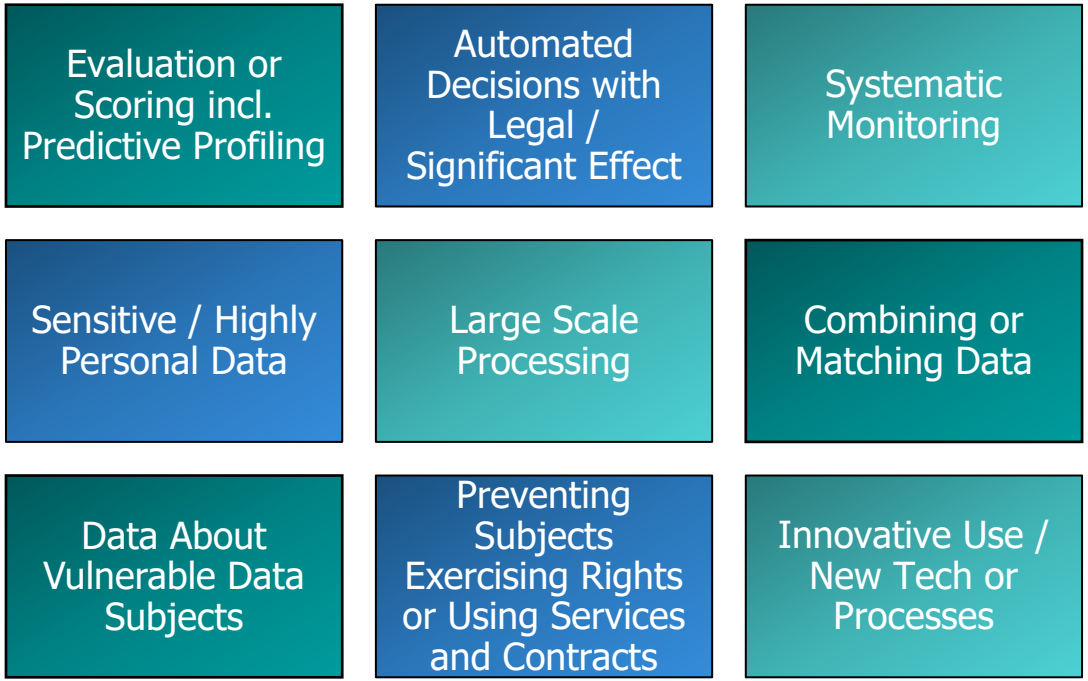


Image credit: 123rf Stock Photo: Serhii Radachynskyi

Do Vs Tool

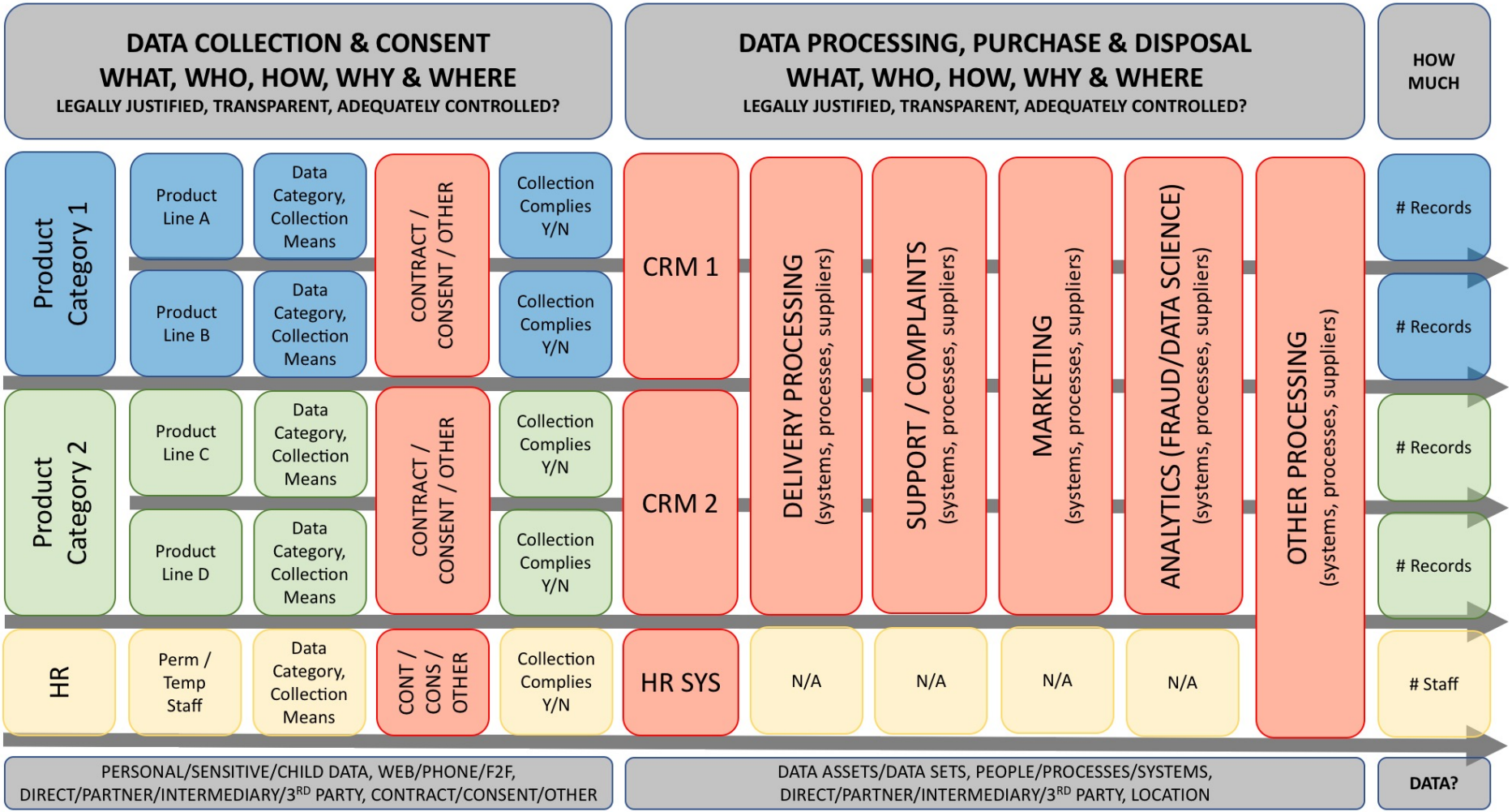
Records of Processing vs an asset inventory





Check inherently risky processing

From Article 29 Working Party, WP 248, Guidelines on Data Protection Impact Assessment, Adopted 4 October 2017.



Revisit your CARDI and RACI

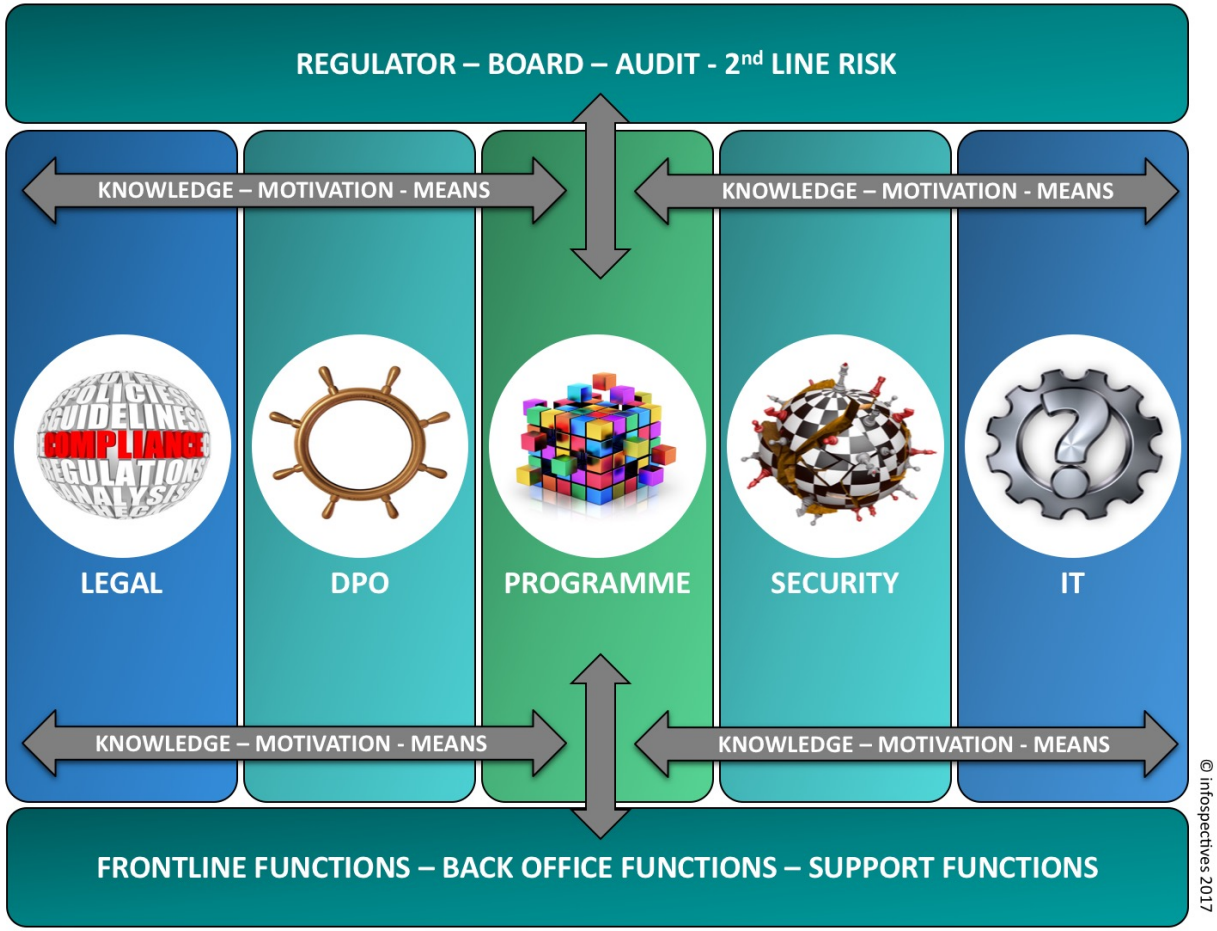


Image credit: 123rf Stock Photo: Bruce Rolff

Image credit: 123rf Stock Photo: Bruce Rolff

Don't boil the ocean

Version 1.0
06/2014

DRAFT - Risk Matrix

Risks	Unjustifiable Collection			Inappropriate Use Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Security Breach Lost Data Stolen Data Access Violation			Aggregate
	Likely	Serious	Score	Likely	Serious	Score	Likely	Serious	Score	Risk Rank
Tangible Harm										
Bodily Harm	0	0	0	0	0	0	0	0	0	**0**
Loss of liberty or freedom	0	0	0	0	0	0	0	0	0	**0**
Financial loss	0	0	0	0	0	0	0	0	0	**0**
Other tangible loss	0	0	0	0	0	0	0	0	0	**0**
Intangible Distress										
Excessive surveillance	0	0	0	0	0	0	0	0	0	**0**
Suppress free speech	0	0	0	0	0	0	0	0	0	**0**
Suppress associations	0	0	0	0	0	0	0	0	0	**0**
Embarrassment/anxiety	0	0	0	0	0	0	0	0	0	**0**
Discrimination	0	0	0	0	0	0	0	0	0	**0**
Excessive state power	0	0	0	0	0	0	0	0	0	**0**
Loss of social trust	0	0	0	0	0	0	0	0	0	**0**

Review your risk matrix

Legend:
Rank 'Likely' from 10 (high) to 1 (low) based on the highest score for any component
Rank 'Serious' from 10 (high) to 1 (low) based on the highest score for any component

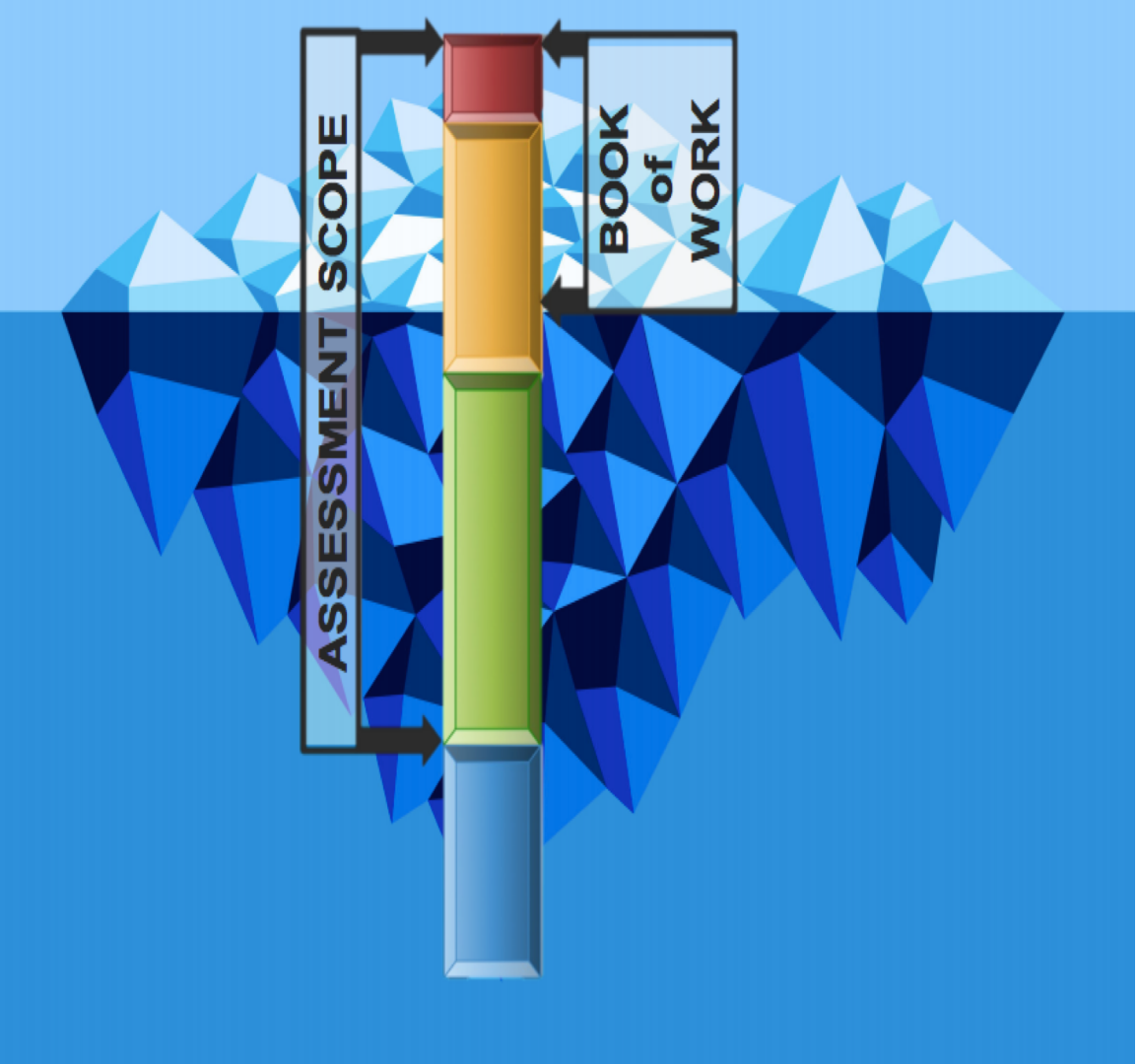
Aggregate Risk Rank:
Highest score is 300
Lowest score is 0

From: Centre for Information Policy Research, Hunton & Williams LLP, A Risk-based Approach to Privacy: Improving Effectiveness in Practice, June 2014

Complying *≠ Managing Risk

*sometimes

Non-compliance **NO impact on data subjects**	Non-compliance **Impact on data subjects**
• Non-compliance identified via audit, incident, or complaint about processing.	• Non-compliance identified via audit, incident, or complaint about processing.
• No impact on rights and freedoms of data subjects +/- other impact on C, I, or A of org. assets.	• Impact on rights and freedoms of data subjects +/- other impact on C, I, or A of org. assets.
• Sanction, fine, or publicity leading to reputation damage	• Sanction, fine, or publicity leading to reputation damage
• loss of customer / client / shareholder confidence	• loss of customer / client / shareholder confidence



Defer edge cases and details


DOCUMENT
EVERYTHING

Fix the Shop Window

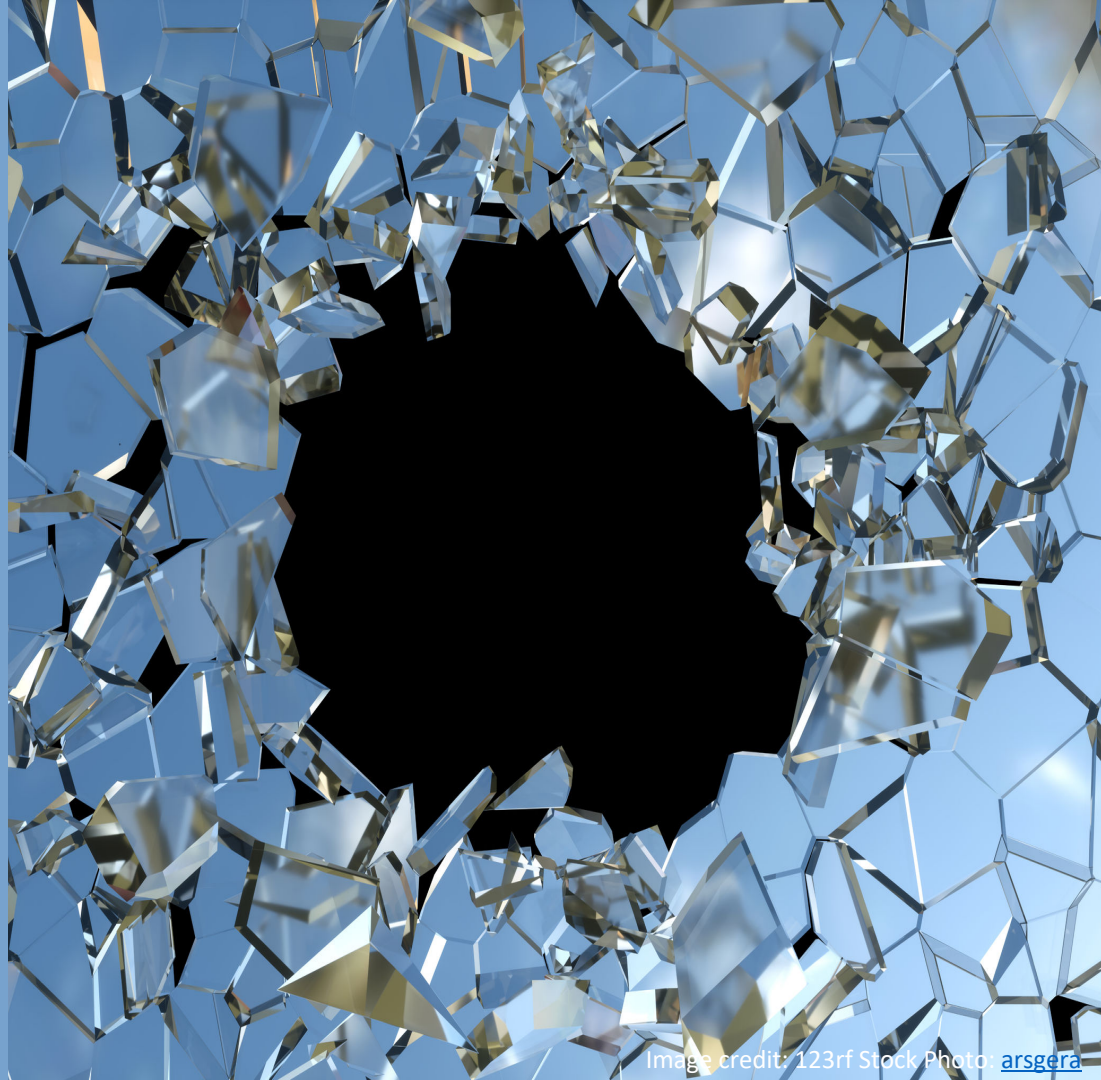


Image credit: 123rf Stock Photo: arsgera

Sort the small subset of new consents

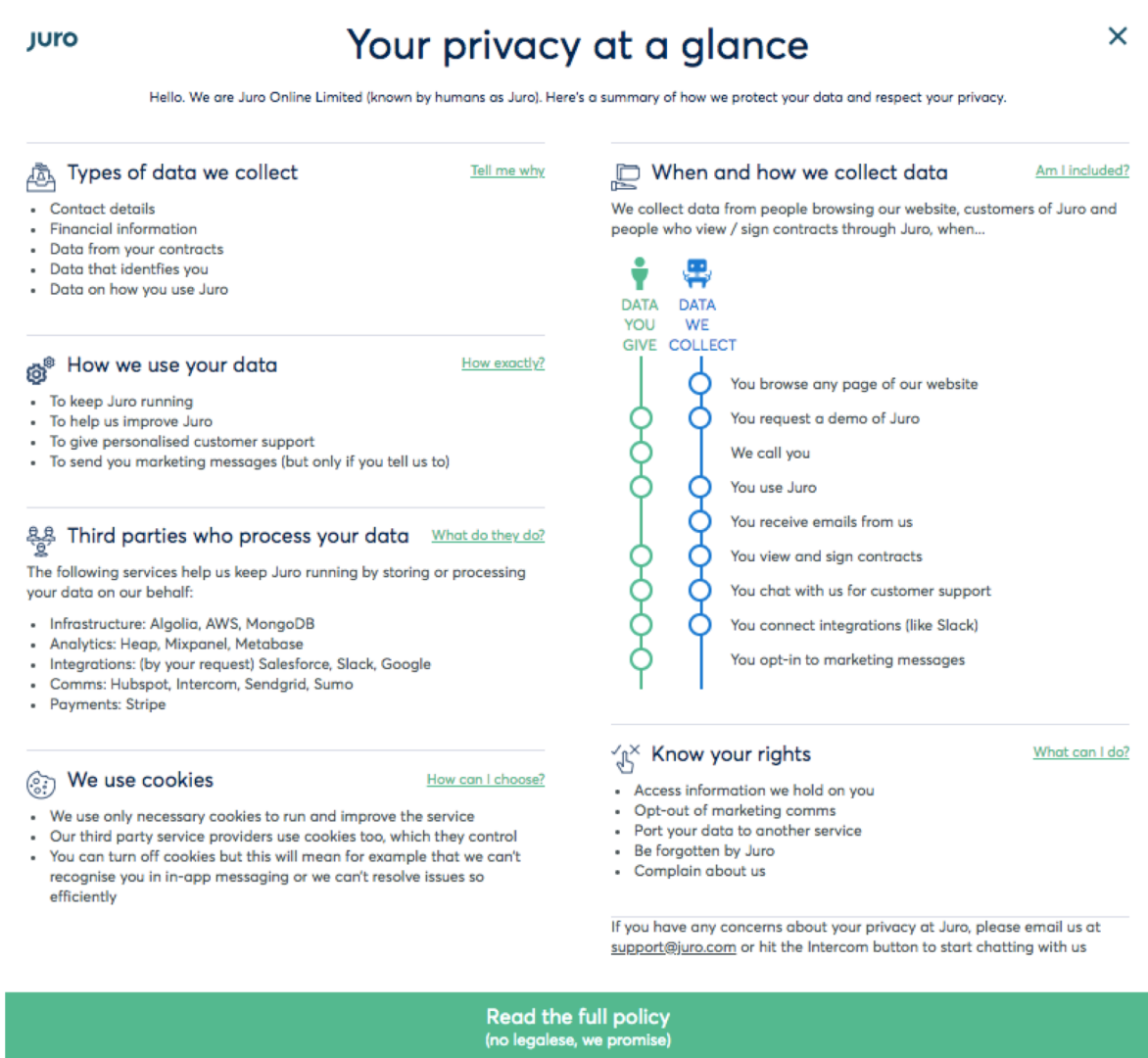
At-a-glance guide to the marketing rules

Method of communication	Individual consumers (plus sole traders and partnerships)	Business-to-business (companies and corporate bodies)
Live calls	☐ Screen against the Telephone Preference Service (TPS) ☐ Can opt out	☐ Screen against the Corporate Telephone Preference Service (CTPS) ☐ Can opt out
Recorded calls	☐ Consumer must have given caller specific consent to make recorded marketing calls.	☐ Consumer must have given caller specific consent to make recorded marketing calls.
Emails or texts	☐ Consumer must have given sender specific consent to send marketing emails/texts. ☐ Or soft opt-in (previous customer, our own similar product, had a chance to opt out)	☐ Can email or text corporate bodies ☐ Good practice to offer opt out ☐ Individual employees can opt out
Faxes	☐ Consumer must have given sender specific consent to send marketing faxes	☐ Screen against the Fax Preference Service (FPS) ☐ Can opt out
Mail	☐ Name and address obtained fairly ☐ Can opt out	☐ Can mail corporate bodies ☐ Individual employees can opt out

ico. Information Commissioner's Office

UK ICO, Direct Marketing Checklist
https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf

Be transparent and clearly communicate the rest



juro

Your privacy at a glance

Hello. We are Juro Online Limited (known by humans as Juro). Here's a summary of how we protect your data and respect your privacy.

Types of data we collect

Tell me why

- Contact details
- Financial information
- Data from your contracts
- Data that identfies you
- Data on how you use Juro

How we use your data

How exactly?

- To keep Juro running
- To help us improve Juro
- To give personalised customer support
- To send you marketing messages (but only if you tell us to)

Third parties who process your data

What do they do?

The following services help us keep Juro running by storing or processing your data on our behalf:

- Infrastructure: Algolia, AWS, MongoDB
- Analytics: Heap, Mixpanel, Metabase
- Integrations: (by your request) Salesforce, Slack, Google
- Comms: Hubspot, Intercom, Sendgrid, Sumo
- Payments: Stripe

We use cookies

How can I choose?

- We use only necessary cookies to run and improve the service
- Our third party service providers use cookies too, which they control
- You can turn off cookies but this will mean for example that we can't recognise you in in-app messaging or we can't resolve issues so efficiently

When and how we collect data

Am I included?

We collect data from people browsing our website, customers of Juro and people who view / sign contracts through Juro, when...

DATA YOU GIVE	DATA WE COLLECT
	You browse any page of our website
	You request a demo of Juro
	We call you
	You use Juro
	You receive emails from us
	You view and sign contracts
	You chat with us for customer support
	You connect integrations (like Slack)
	You opt-in to marketing messages

Know your rights

What can I do?

- Access information we hold on you
- Opt-out of marketing comms
- Port your data to another service
- Be forgotten by Juro
- Complain about us

If you have any concerns about your privacy at Juro, please email us at support@juro.com or hit the Intercom button to start chatting with us

Read the full policy
(no legalese, we promise)

Privacy notice from www.juro.com ©Juro Online Ltd

On May 25th 2018

Staff need to know what to say before someone calls


…and if you
can't comply…

The GDPR Sniff Test

(If it smells bad it probably is)

You know what the privacy notice says vs data handling reality

- If it was your data, would the privacy notice feel easy to read and transparent about planned data use?
- If it was your data, would planned use feel necessary and proportionate?
- When processing isn't necessary to deliver products and services, do you get a choice?

You know what the data security risks are vs control reality

- If it was your data, would the security controls in place feel appropriate, and adequate to mitigate unacceptable risk to you and your contacts?

You know the justifications vs reality of potential impact on data subjects

- If it was your data, would the stated organisational interests feel like they outweigh all the things that could go personally and cumulatively wrong?

Stop and/or report the risk

Risks	Acceptable/can be improved on?	Corrective controls	Residual severity	Residual likelihood
Illegitimate access to data	*[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]*	*[Where applicable, he shall indicate here any additional controls that would prove necessary.]*		
Unwanted change of data	*[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]*	*[Where applicable, he shall indicate here any additional controls that would prove necessary.]*		
Disappearance of data	*[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]*	*[Where applicable, he shall indicate here any additional controls that would prove necessary.]*		

From CNIL Privacy Impact Assessment Template https://www.cnil.fr/en/PIA-privacy-impact-assessment-en, Feb, 2018

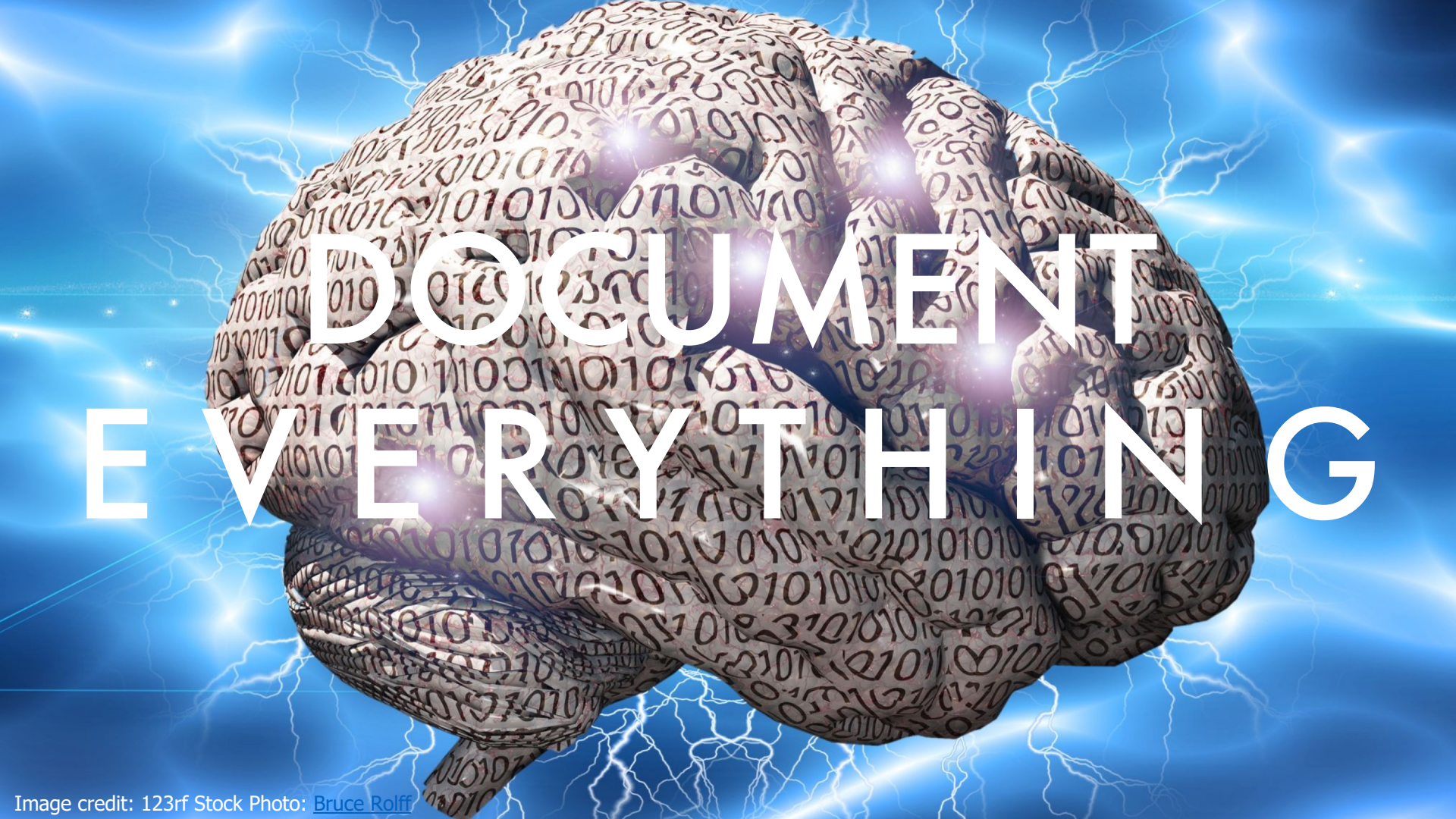


Image credit: 123rf Stock Photo: Bruce Rolff

Strengthen foundations, manage risks, and carry on