



# ProPolicies

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



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

Dynamic Privacy Compliance Policies creation software  
Create required compliant policies in minutes



# ProPolicies

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



Contact :

[info@propolicies.com](mailto:info@propolicies.com)

[info@gdpr.ie](mailto:info@gdpr.ie)



ProPolicies



# What is needed to demonstrate compliance with Irish Data Protection Act and GDPR.

# Today's Topics

- Introductions
- Data Protection In the news
- The Legislation - a brief overview
  - Principles of Privacy ( GDPR and Irish DPA)
  - Accountability and Implications for controller and processor
- Why and how to Comply?
- Required Policies, Evidence and Processes under Irish DPA and GDPR
- ProPolicies – and SCSi what we do to help
  - How to create and personalise your policies and procedures
- Free advice and links

# Housekeeping

If you have any questions please ask

But Preferably keep them to the end

# Introductions

## Who am I?

## What I can't do today!

I am not offering legal advice.

All data protection guidance provided is provided in good faith but without warranty of any kind.

# Data Protection In The News





[About the ICO](#) / [News and events](#) / [News and blogs](#) /  
Estate agency fined £80,000 for failing to keep tenants' data safe

## Estate agency fined £80,000 for failing to keep tenants' data safe

**Data of Foxtons Group customers leaked by hackers on the dark web – and they did not tell people at risk**  
**February 2<sup>nd</sup> 2021**

[Action we've taken](#) / [Enforcement](#) / [Black Lion Marketing Ltd](#)

## Black Lion Marketing Ltd

Date **27 March 2020**  
Type **Monetary penalties**  
Sector **Marketing**

Black Lion Marketing Ltd fined £171,000 for making unsolicited direct marketing

[Action we've taken](#) / [Enforcement](#) / [Pension House Exchange Limited](#)

## Pension House Exchange Limited

Date **09 December 2020**  
Type **Monetary penalties**  
Sector **Marketing**

The Information Commissioner's Office (ICO) has fined Pension House Exchange Limited has been fined £45,000 for making 39,722 connected unsolicited calls for the purposes of direct marketing in relation to occupational pension schemes or personal

[Action we've taken](#) / [Enforcement](#) / [Smart Home Protection Ltd](#)

## Smart Home Protection Ltd

Date **13 June 2019**  
Type **Monetary penalties**  
Sector **Land or property services**

The Information Commissioner's Office (ICO) has fined Smart Home Protection Ltd £90,000 for making nuisance calls to people registered with the Telephone Preference Service (TPS).



# Data Protection in the News

- Berlin property company Deutsche Wohnen was fined more than **€14.5m** due to a GDPR breach.
  - The company is reported to have **retained old customer data**, which is a breach of administrative obligations, rather than a data breach which is loss or misuse of customer data.
- London Estate agency fined **£80,000** - failing to keep tenants' data safe
  - The Information Commissioner's Office (ICO) fined a London estate agency £80,000 for leaving 18,610 customers' personal data exposed for almost two years. .Jul 19, 2019

# Data Protection in the News

- French real estate company fined **€400,000** for GDPR violations
  - French data protection authority CNIL levied a €400,000 fine on Sergic, a French real estate services provider, for failing to adequately protect the data of users of its Website and for **implementing inappropriate procedures for storing data** in violation of the EU's General Data Protection Regulation (GDPR).
- **Non news items**
  - **Phishing attacks**
  - **Email redirects and takeovers**
  - **Eprivacy Fines – communication preferences**

# GDPR and Irish Data Protection Act Overview

So What's it all  
about?

# 10 December 1948

## Universal Declaration of Human Rights

Over **70** years ago!

### Article 12

No one shall be subjected to arbitrary interference with **his privacy, family, home or correspondence**, nor to attacks upon his honour and reputation. Everyone has the **right to the protection of the law** against such interference or attacks.

# GDPR and Irish DPA Overview

Replaced existing laws from **25<sup>th</sup> May 2018**

It is a Regulation therefore **directly effective**

intended to **harmonise privacy laws**, with some  
Member State legislation

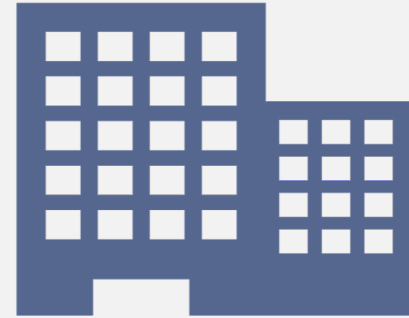
# GDPR Overview



**Mandatory**



Applies to  
**ALL**  
companies



Imposes  
obligations



Demonstrate  
and Evidence  
Compliance

# GDPR Overview



## Citizen Rights enhanced, harmonized and extended

- Requirement for **consent** to be a freely given, specific, informed and unambiguous indication of wishes
- Give or withdraw data specific consent or portions
- **Informed of types of processing**
- **access to / rectify / erase / object to processing**
- Insight in automatic decision making
- **Transfer personal data to other provider (portability)**



## Broadened scope 'Personal Data'

- All direct and indirect identifiers
- Behavioral-, derived- and self-identified data
  - Physical
  - Genetic
  - Cultural
  - Social
  - Economic
- Format and technology agnostic



## Organizational Impact

- **Data controller and data processors liable for breaches**
- Data controllers legally bound to validate data processor's compliance – **Eg CRM**
- Data Protection Officer
- **Stringent data security & breach management**
- Conditions for cross-border data transfer altered
- **Requirement to demonstrate compliance**



## Increased cost of non-compliance

- **Fines up to 4% of annual turnover or 20 million Euros whichever is greater**
- Data Privacy Authorities empowered
- Increased activist and court activity – **Civil remedies**
- **Risk / "Cost" of reputation loss**



# Data Protection Principals

There are only 7

# Principles of the GDPR (article 5)

1. Processed lawfully, fairly and in a transparent manner in relation to individuals (TRANSPARENCY)
2. Collected for specified, explicit and legitimate purposes  
(PURPOSE LIMITATION)
  - and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

# Principles of the GDPR (article 5)

## 3. Adequate, relevant and limited (DATA MINIMISATION)

- to what is necessary in relation to the purposes for which they are processed;

## 4. Accurate and kept up to date; (ACCURACY)

- every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

# Principles of the GDPR (article 5)

## 5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- **STORAGE LIMITATION**

- personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures (TOMS) required by the GDPR in order to safeguard the rights and freedoms of individuals;

# Principles of the GDPR (article 5)

6. Processed in a manner that ensures appropriate security of the personal data,
- SECURITY AND CONFIDENTIALITY
  - including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

# Principles of the GDPR (article 5)

## 7. **Accountability:**

The final principle

and a new principle under the GDPR, states that

organisations must take responsibility for the data they hold and demonstrate compliance with the other principles.

# Principles of the GDPR (article 5)

“the **controller** shall be **responsible for, and be able to demonstrate,** compliance with the principles”

Article 5(2)



# Principles of the GDPR (article 5)

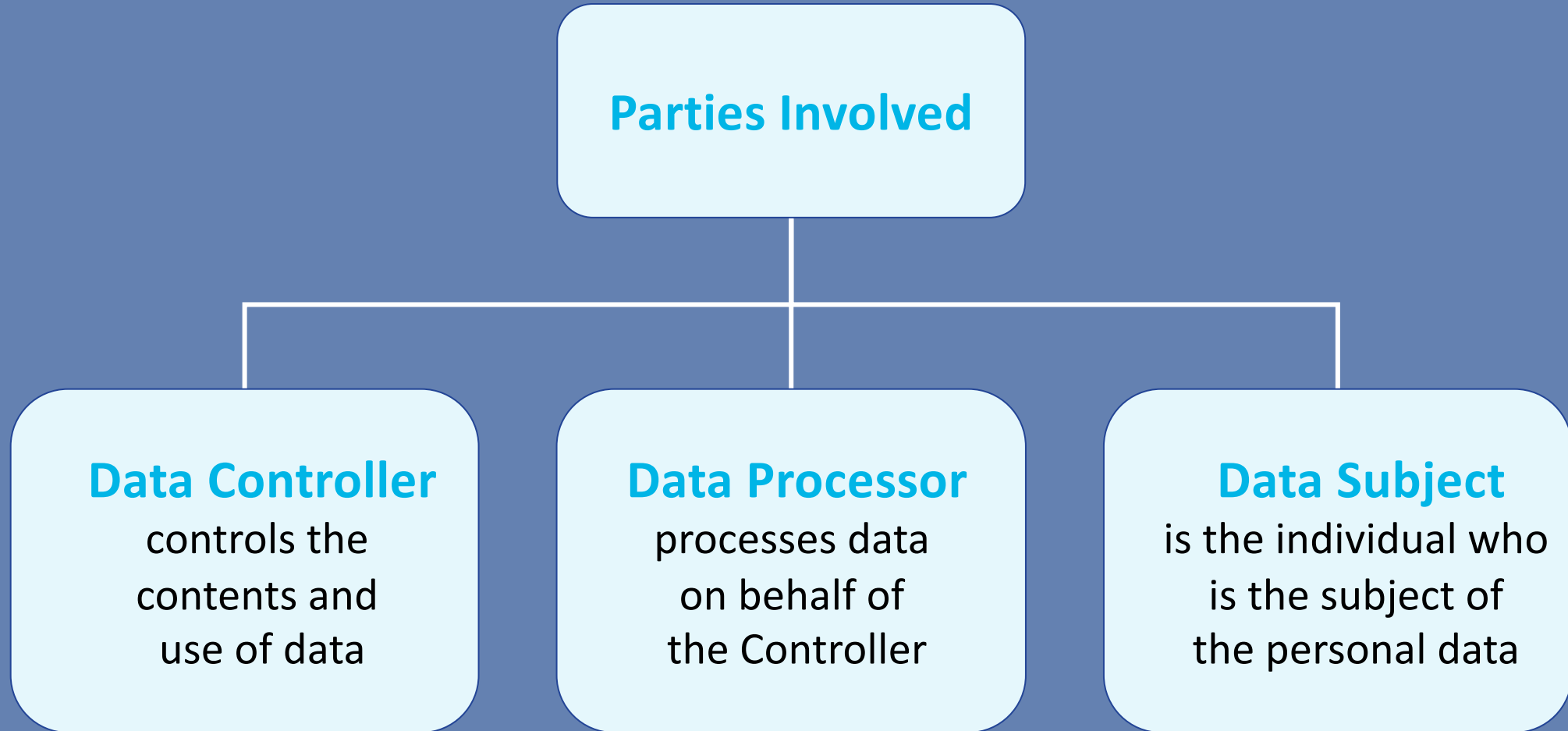
Organisations must be able to evidence the steps they have taken to demonstrate compliance.

This could include:

- **Evaluating** current practices ( Audit/ gap analysis)
- **Creating** required privacy/Data protection Policies and procedures
- **Creating** records of processing activities – where required
- **Raising Awareness** – training staff on privacy principles, processes , policies
- **keeping training records**
- **Obtaining appropriate consent** – and maintaining evidence (where required)
- Integrating **Privacy by design (PbD)** and Carrying out **Data Protection Impact Assessments (DPIA)** on new processing - where required

# Some helpful Definitions

# GDPR Overview



# Controller

Means a natural or legal person, public authority, agency or other body who, alone or jointly with others, **controls the purposes and means** of processing of the personal data.

## Key Aspects

- Primary focus for compliance obligation
- Must be identifiable
- Has a statutory duty to the data subject
- 'ownership' of the data is not required
- Increased scope of the GDPR



# Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller

**There must be a formal, written contract** with terms as set out in the GDPR between the controller and processor

‘Processor’ does not include persons under the direct control of a controller or processor, such as employees.

- Key aspects
  - ◊ **Activities must be governed by contract;**
  - ◊ Can be a controller as well, or become one;
  - ◊ Can be liable if it acts outside of or contrary to the controllers instructions, OR is in breach of its own obligations under GPDR.



# GDPR Overview

## Process

Performing any operation  
on personal data,  
including obtaining it,  
storing it or disclosing it

## Disclose

Passing personal data  
between legal entities  
i.e. different companies  
or people

## Transfer

The passing of personal  
data across  
jurisdictions

# REMINDER



# Principles of the GDPR (article 5)

“the **controller** shall be responsible for, and be able to demonstrate, compliance with the principles”

Article 5(2)

# Types of Data Collected by Property Professionals

- Customer /client data – Vendors – Purchasers – Tenants – Landlords
- AML records – Required retention periods
- Financial records etc
- Consent data – marketing, sales and lettings
- Employment records
- Suppliers and third party details
- Potential sensitive health data ( COVID) in addition to normal HR data

# Types of Data Collected by Property Professionals

- **Have you clearly informed the data subjects, customers and employees**
- **(Privacy statement, etc)**
  - What you are collecting , Why are you collecting it
  - How long do you need to hold it
  - Who you share it with
  - What security measures you have in place
  - Their rights and how to exercise them
- **Is your collection Adequate, relevant and not excessive and can you prove it?**
  - **Adequate** -
    - Principle of data minimisation means you should Gather and hold only the data you need.
  - **Relevant** -
    - Personal data sought and kept by data controllers should be sufficient to enable them to achieve their specified purpose(s) and no more.
  - **Not excessive** –
    - Don't collect more than is required by Regulation or to complete the task.

# Types of Data Collected by Property Professionals

- **Data controllers (Property Professionals)** have **no basis for collecting or keeping personal data that they do not need.**
- You can not collect or keep any data on the off-chance that it might be useful in the future.
- Have all appropriate policies, procedures and documentation in place and ensure all you staff are aware of their roles and responsibilities

# Types of Data Collected by Property Professionals

- Examples:-
- **Rental viewings** –
  - **Example** - PP may have to take references off each person –
  - They should explain that they only retain the references, copies of ID etc until the tenancy of the property is signed and then explain that they will destroy those collected that were not successful
- **Sales process and Viewings.**
  - **Example** - Data Subjects details should only be retained if the Data Subject (Viewer) has given consent and they want to register their interest in a property or be listed for future property for sale/rent.
- **Proof of loan** – might be sought for top 2/3 serious bidders –
  - Once you have seen evidence of this there is no need to retain a copy of this personal information. Main thing is always be clear to the customer on your processes- and have proof
- **Your Retention Policy** should clearly outline retention periods for categories of personal data you collect and hold. (e.g. What is your legal basis for retention?)

# REMINDER

# Principles of the GDPR (article 5)

“the **controller** shall be responsible for, and be able to demonstrate, compliance with the principles”

Article 5(2)



# Some Policy / Evidence Areas in more detail

# Data Subject Rights

Focus is on the rights of the data subject

Article 12:	Exercise of the Rights of the Data Subject
Article 13 & 14:	Right to Be Informed
Article 15:	Right to Access
Article 16:	Right to Rectification
Article 17:	Right to Erasure (“Right to be Forgotten”)
Article 18:	Right to Restriction of Processing
Article 19:	Notification Obligation
Article 20:	Right to Data Portability
Article 21:	Right to Object to Processing
Article 22:	Right to Object to Automated Individual Decision Making
Article 7(3):	Right to Withdraw Consent


# Data Subject Rights

- Right to complain to the Supervisory Authority
- Right of judicial remedy against decision of Supervisory Authority
- **Right to compensation through the civil courts**

# Data Subject Rights

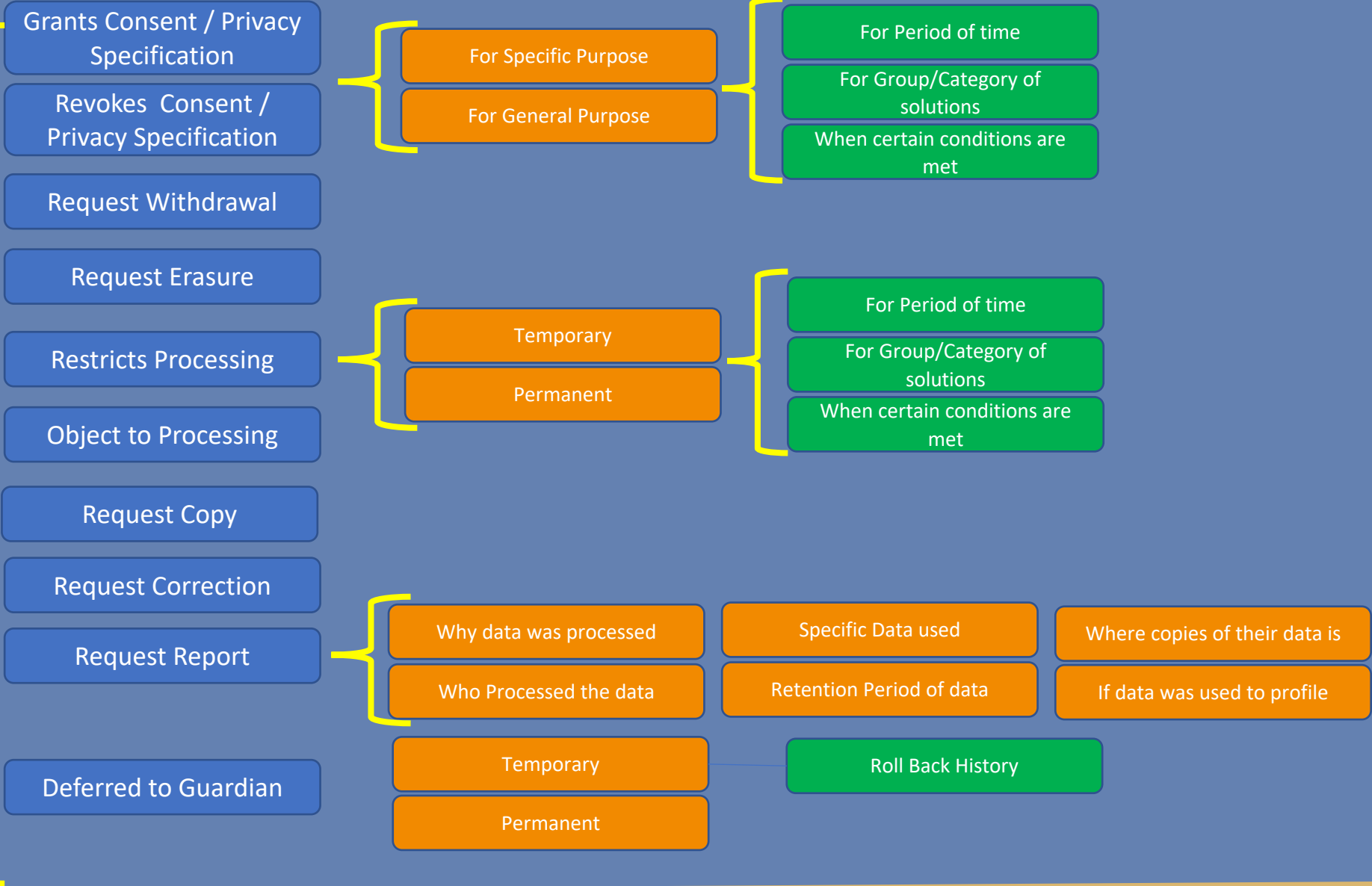
These GDPR Articles have also created new **operational requirements for controllers** to

- “**facilitate**” the requests (Art 12(2); Rec 59)
- “**electronically**” (Art 12(1), (3); Rec 59),
- **within a specified time-period** (Art 12(3); Rec 59),
- **demonstrable record keeping** (Art 5; Rec 39)
- and **clear communication** (Art 12(1); Rec 58).



# Data Subject

## SUBJECT RIGHTS



# Data Collection & Retention

- know what personal data you hold and why you need it.
- Carefully consider and justify how long you keep personal data.
- Have a **Retention policy** with standard retention periods (**schedule**), in line with documentation obligations.
- Regularly **review** your information and erase or anonymise personal data when you no longer need it.
- Have **DSAR policy** and appropriate **processes in place to comply with individuals' requests** for erasure under 'the right to be forgotten'.
- Clearly identify any personal data (if any) that you may need to **retain** for public interest archiving, scientific or historical research, or statistical purposes.

## LEGAL FILES AND PAPERS

# Data Collection & Retention

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	10 years after close of matter
Litigation Files	10 year after expiration of appeals or time for filing appeals
Court Orders	Permanent
Requests for Departure from Records Retention Plan	10 years

## PERSONNEL RECORDS

Record Type	Retention Period
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	6 years after departure
Employment Contracts – Individual	7 years after departure

# Data Collection & Retention

## ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank Statements and Cancelled Cheques	7 years
Employee Expense Reports	7 years
General Ledgers	Permanent
Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years



# Data Collection & Retention

## TAX RECORDS

Record Type	Retention Period
Tax-Exemption Documents and Related Correspondence	Permanent
Tax Bills, Receipts, Statements	7 years
Tax Returns - Income, Franchise, Property	Permanent
Tax Workpaper Packages - Originals	7 years
Sales VAT Records	7 years

# Client Communications - PECR

- ePrivacy – email marketing and GDPR
- Always obtain informed consent for text, email, phone etc
- Always have a record of this
- Always give an “opt out” on all communications
- Have a clear enforcement method and evidence
- Useful Guidance from UK ICO
  - <https://ico.org.uk/for-organisations/guide-to-pecr/>

# Why Comply

It's the law

It's your reputation

Non compliance can cost the business dearly

# How to Comply

# How to Comply

In order to be able to demonstrate compliance you need to have : -

- **Privacy Notice/Policy (articles 12,13,14)**
- **Data Protection Policy (article 24)**
- **Compliant cookie notice** and set of **controls** and evidence of consent
- **Records of Processing Activities ROPA** (article 30) - where required
- **Data retention policy**, schedule and enforcement evidence (5,13,13,30)
- Policy and procedures for all subjects' rights including release of information for **DSAR's (Data Subject Access Requests) (12-22)**
- **Train your staff**, make them aware – keep records of training

# How to Comply

In order to be able to demonstrate compliance you need to : -

- Have **GDPR Compliant contracts** with all data processors (28, 32, 82)
- Have **data breach management policy and notification procedures** (4,33,34)
- Keep a **Breach log/register** of all breaches and “near misses” (33)
- Implement **privacy by design** for all new processing of personal data (25)
- Demonstrate that you consider the privacy of the individual at all times using **DPIA** threshold assessments and full **DPIA** where required (35)
- Document all the **privacy and security precautions** you have in place (32)

# How to Comply

## Other Policies that you may require

- CCTV policy
- Clear desk policy
- Covid-19
  - Add to / updates to policies to reflect health data linked to Covid
  - BYOD (Bring Your Own Device) policy
  - Remote Working Policy
- Lastly **BREXIT IMPLICATIONS** – Data Transfers and EU REPRESENTATIVES

# Remember

Policies alone do not make  
you compliant

You also need to  
Create Awareness and train your staff ( And evidence this)

Have processes and procedures, documentation, logs, evidence

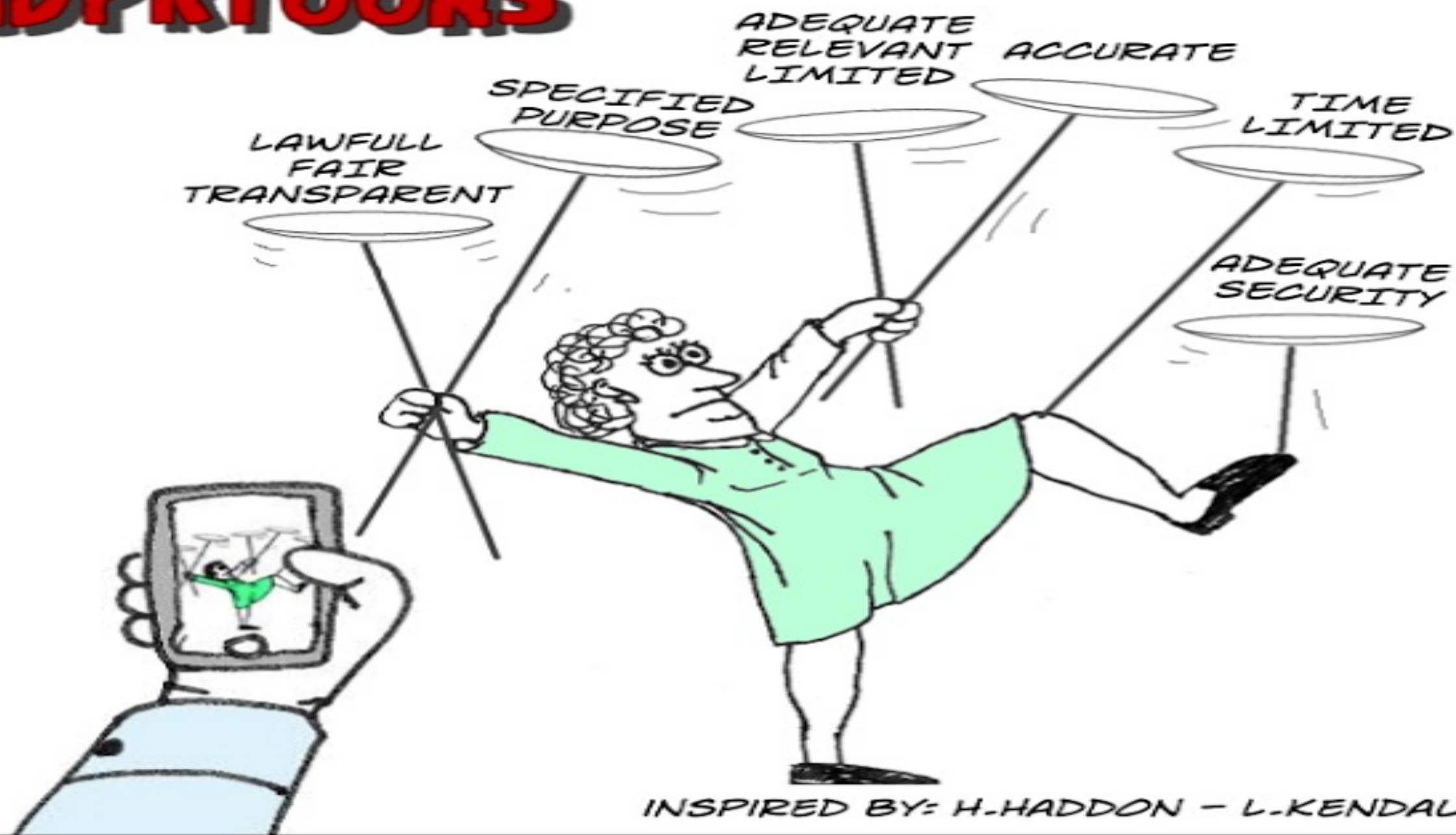


# ITS ALL ABOUT EVIDENCE

- AND IT'S A TOUGH JOB!

# GDPR TOONS

COPYRIGHT 2017 B.DREYER GDPRTOONS.COM



INSPIRED BY: H.HADDON - L.KENDALL

So who is  
responsible  
for Data  
Protection ?



# Challenges for Property Service Providers

Time

Understanding of what's required

Knowing how to evidence compliance

Knowing how to maintain compliance

Lack of In house skills

Perceived Prohibitive Costs

Our experience to date

# What Now for you ?





# Good News

# We are here to help



## IMPROVE YOUR GDPR COMPLIANCE EVIDENCE TODAY

### Create Mandatory GDPR & Data Protection Policies for your business

SCSI Member firms can avail of this exclusive offer from ProPolicies to enable them create 20 + different Privacy and Compliance Policies for their business so they can evidence compliance with the GDPR and Data Protection Act 2018.

Our team are ready to help you – Buy now or request a demo.

#### SCSI MEMBER FIRM OFFER

**55% DISCOUNT – ONLY €500 P/A**

Package Normally €1,100 P/A

- Create, customise and download 20+ Policies –
- Simple to use online platform
- Built in Guidance documents, Videos and Tutorials
- Comprehensive GDPR Action Plan for use in your business
- **Free** updates and additions to all policies when guidance/legalisation changes
- Payment choices: Credit Card / Bank Transfer / Invoice

✉ Request Demo

🛒 Annually €500



<https://www.propolicies.com/scsi/>



**ProPolicies**

Members **Discounts of 55%**

**That's just €500 for all required core policies in 2021**

Simple to use Online platform

Create, Personalize and Download your compliant policies

Policies automatically updated when legislation changes or new guidance issued

Eg. Brexit, Schrems , Adequacy decisions etc

Additional services such as consultancy, audits, training will also be available.

<https://www.propolicies.com/scsi/>



Members **Discounts of 55%**

**That's just €500 for all required core policies in 2021**

[info@propolicies.com](mailto:info@propolicies.com)

Thank You

Any Questions?