An Coimisiún um Chosaint Sonraí
Data Protection Commission

Personal Data Breaches

4th April 2019

EDPS-ENISA Conference

Panel Discussion 1 – Experience in Ireland

Introduction –

- **Legislative Frameworks**
- **Data Breaches – definitions, statistics**
- ***Notification* and *Communication* of Personal Data Breaches**
- **Consequences**
- **Key Messages from the DPC**

Niall J. Cavanagh
Assistant Commissioner

The Data Protection Commission

Legislative Frameworks

- **General Data Protection Regulation**
- **Law Enforcement Directive**
- **Data Protection Act 2018**
- **[Data Protection Acts 1988 and 2003] – s.8 of 2018 Act**
- **Statutory Instrument No. 336 of 2011 (e-Privacy Regulations)**

Technical and organisational measures

- Secure the ICT

- Secure the environment/paper based systems

What is a Breach?

Legislative Frameworks

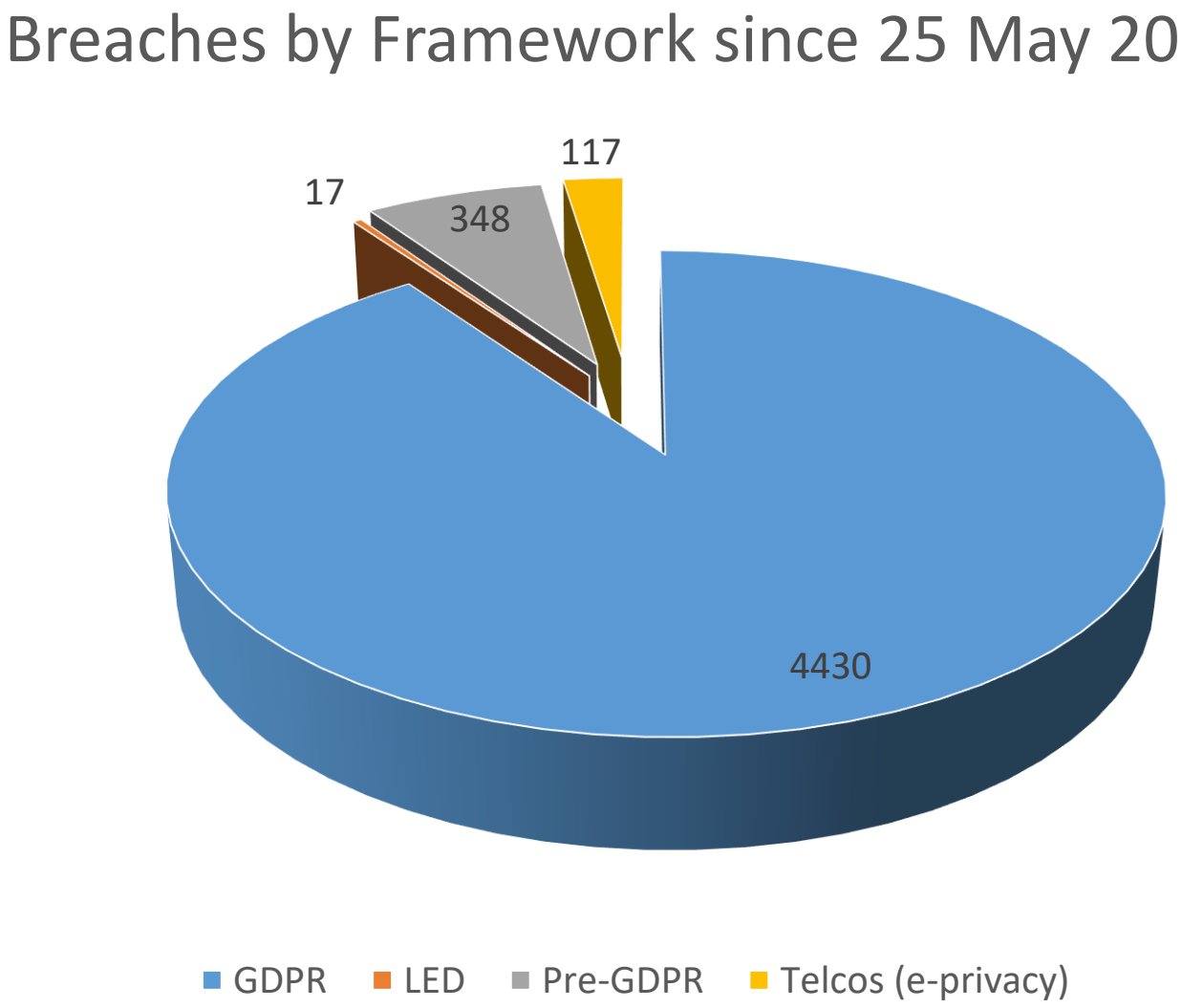
- **General Data Protection Regulation & LED**

  a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

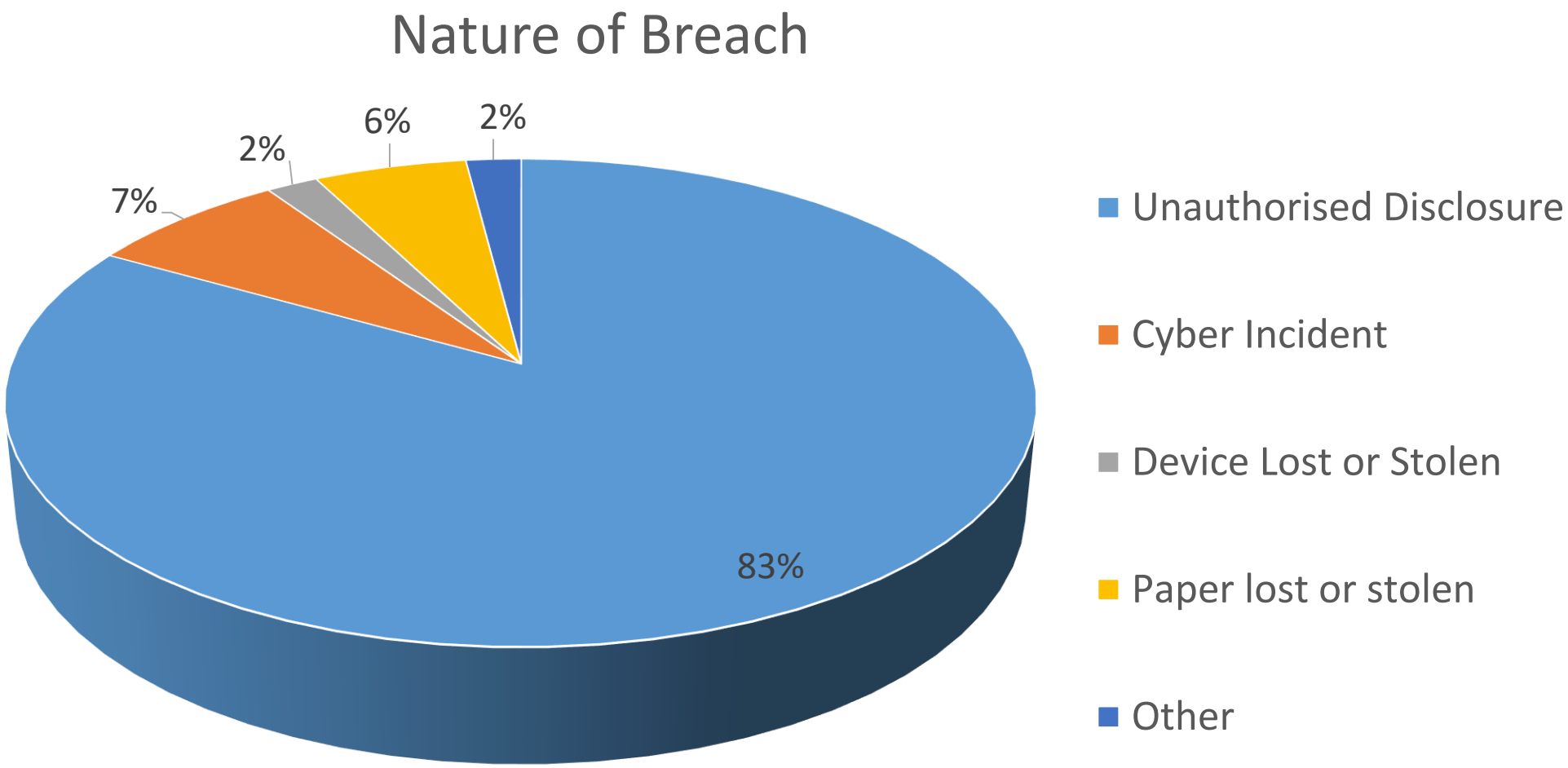
- **Statutory Instrument 336 of 2011 (e-Privacy Regulations)**

  a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Union;

Personal Data Breaches

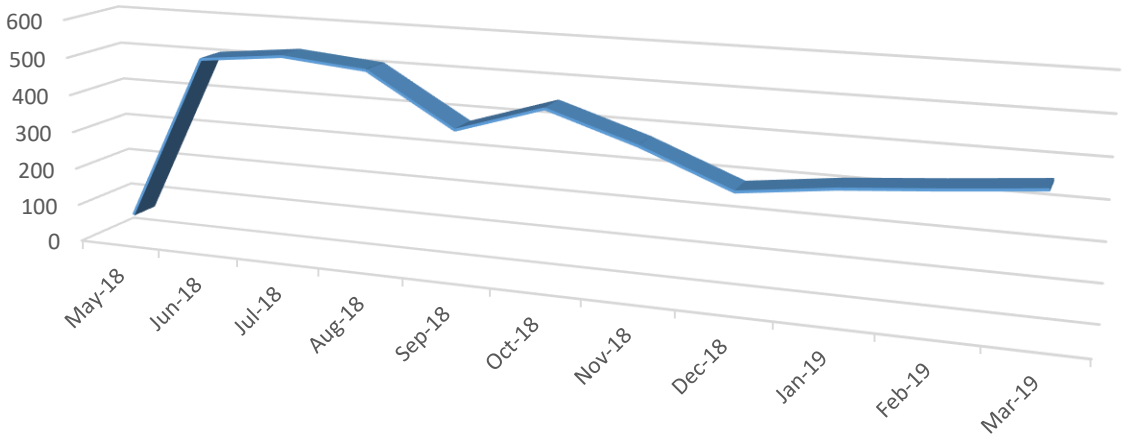


Personal Data Breaches

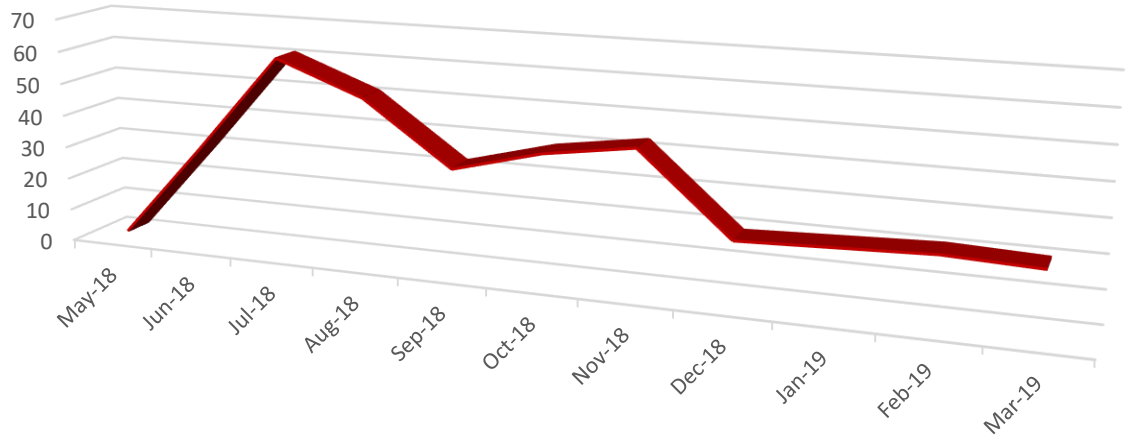


Personal Data Breaches

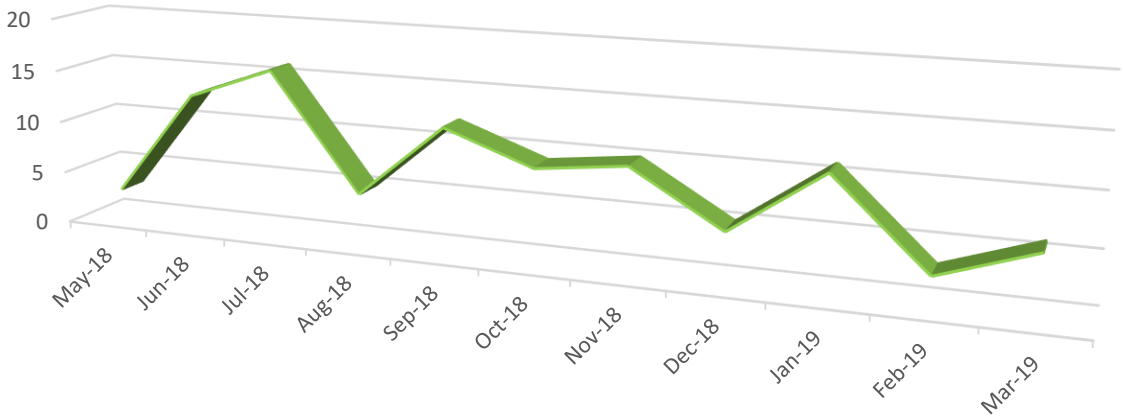
Unauthorised Disclosure



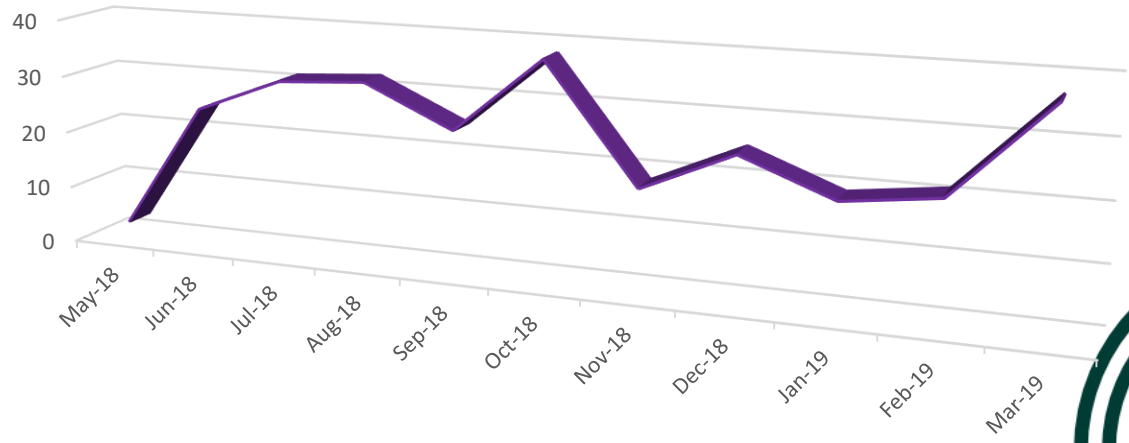
Cyber Incident



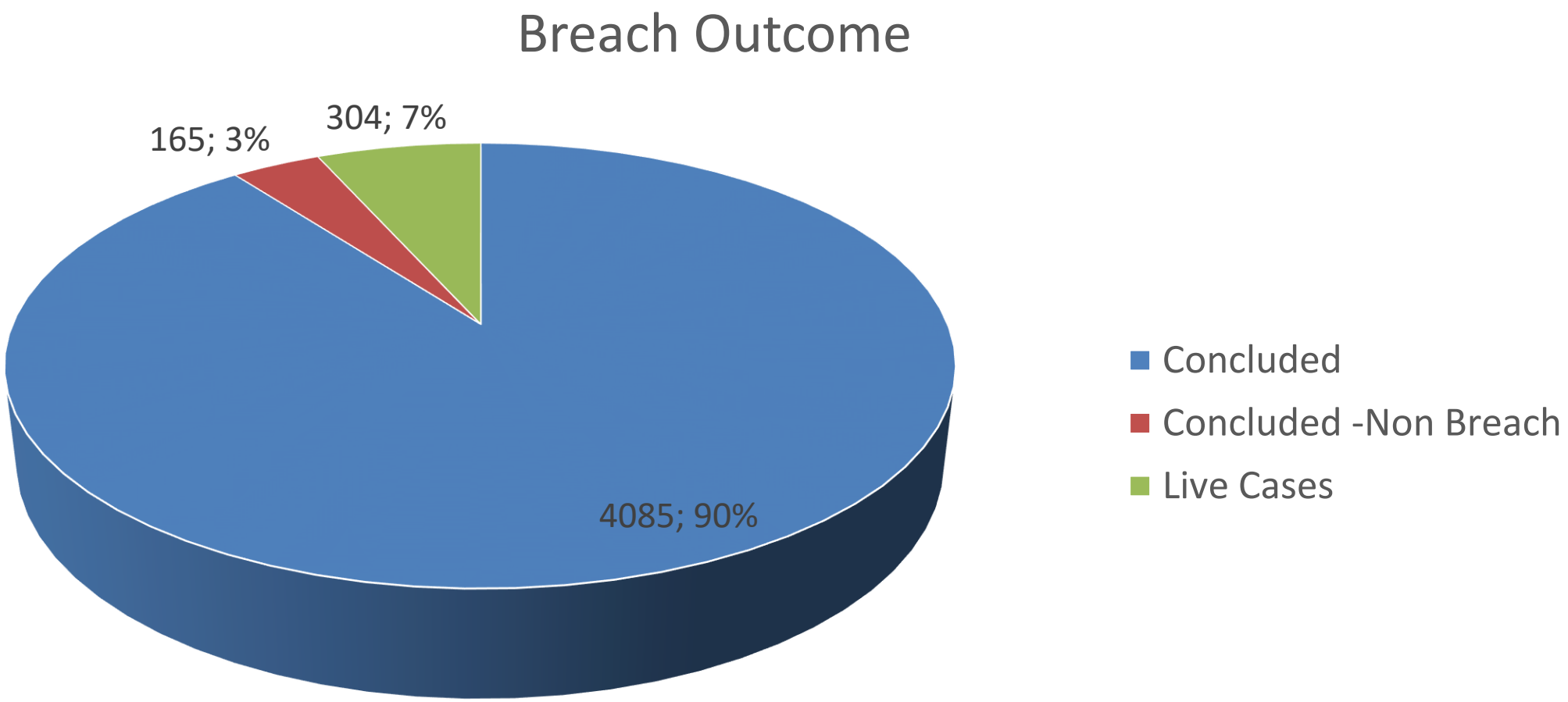
Device Lost or Stolen



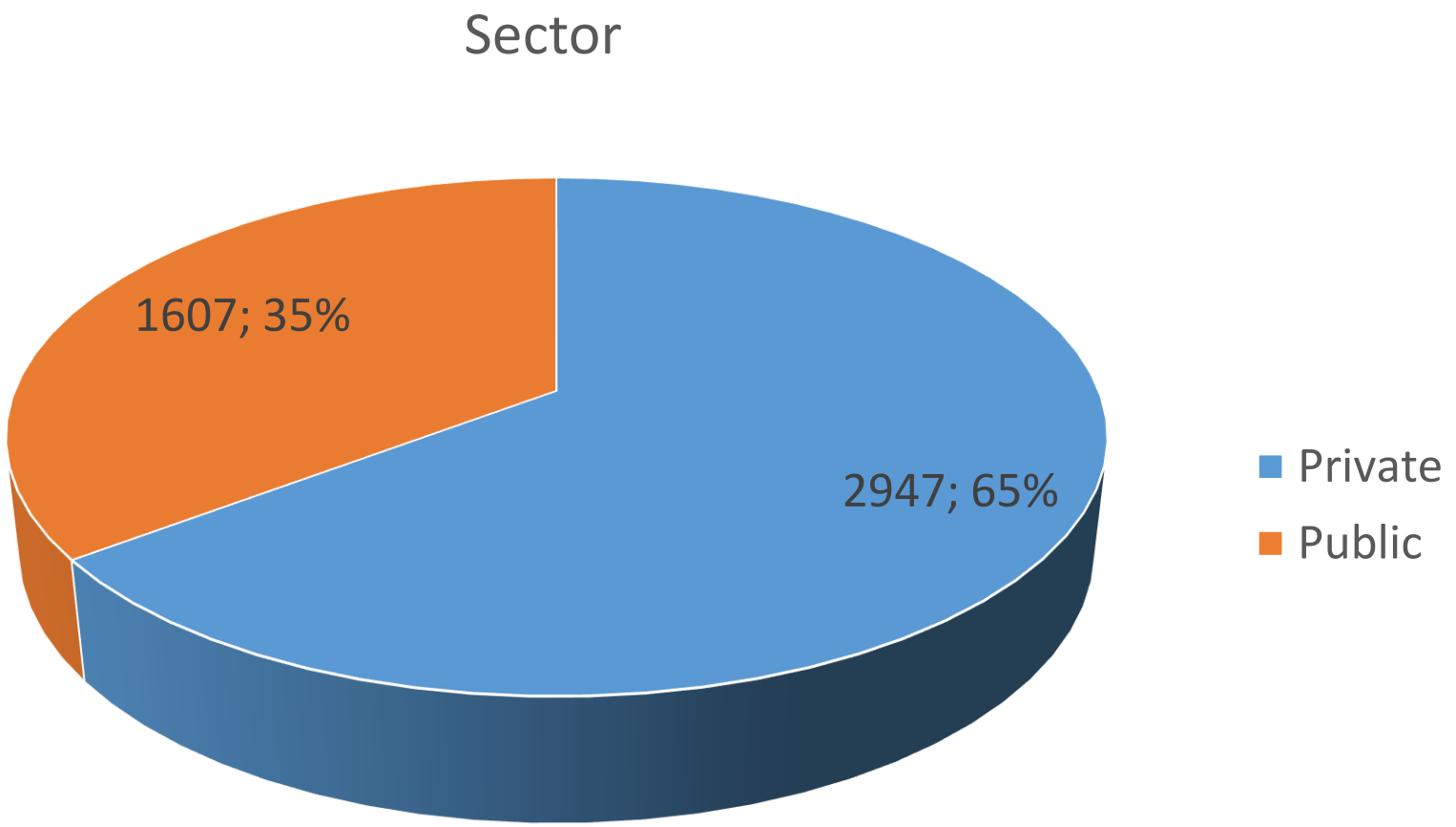
Paper Lost or Stolen



Personal Data Breaches



Personal Data Breaches



Notification to DPC

- **General Data Protection Regulation (Art. 33)**
- **Law Enforcement Directive (s.86 Data Protection Act 2018)**
- **e-Privacy Regulations**

  (S.I. No. 336 of 2011 and

  Commission Regulation (EU) No 611/2013)

Notification/Communication Risk Assessment (all frameworks)

Two steps

1. Notify DPC

   GDPR & LED: *unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons*

   ePrivacy: Always

2. Communicate with Data Subject – (exceptions apply)

   GDPR & LED: if there is likely to be a *high* risk to the rights and freedoms

   ePrivacy: if the breach is *likely to adversely affect the personal data or privacy of a subscriber or individual*

Verification of Risk Assessment (GDPR)

Case Officer evaluates the self declared risk using

- Qualitative Checklist
- Quantitative Risk Assessment tool

Verification of Risk Assessment (GDPR)

Qualitative Check list

Informed by fields of web based notification form:

Description of the breach incident:					
Was the breach reported within 72 hours of awareness?				Yes / No	
If not, is the explanation given for the late notification feasible / reasonable?				Yes / No / Questionable	
Is the possibility of the above processing:				Tick as appropriate ☑	
Giving rise to...		Revealing...		Evaluating/analysing/predicting the following (in order to create/use personal profiles)...	
Discrimination		Racial or ethnic origin		Performance at work	
Identity theft		Political opinions		Economic situation	
Reputation damage		Trade union membership		Location / movements	

Verification of Risk Assessment (GDPR)

Loss of confidentiality		Health data		Reliability / behaviour / health	
Loss of data protected by official secrecy		Religion or philosophical beliefs		Personal preferences / interests	
Other significant economic or social disadvantage		Criminal convictions / offences			
Loss of rights or freedoms		Related security measures			
Loss of control over data		Genetic data			
Financial loss					

Are vulnerable people affected?	Yes / No
Number of persons affected?	[Insert]
Large amount of data affected?	Yes / No
Have the risks to the DS as identified been mitigated...	
• Sufficiently	Yes / No / Questionable
• In a timely manner	Yes / No / Questionable
• Have data subjects been informed?	Yes / No / Questionable

Verification of Risk Assessment (GDPR)

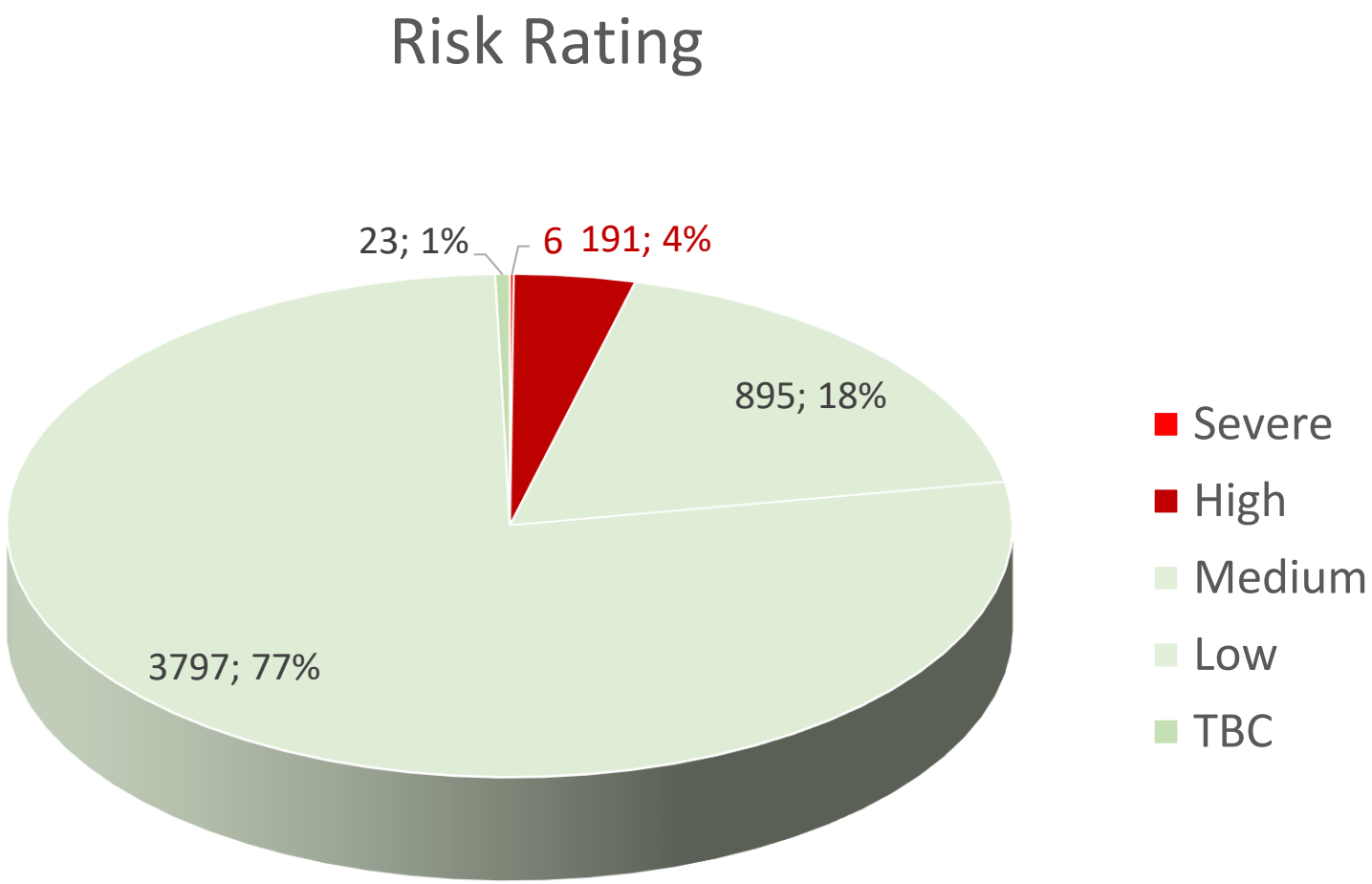
Has the DC/DP identified the organisational / technical deficiencies which led to breach?	Yes / No / Questionable
Have sufficient organisation / technical measures been implemented to address deficiencies identified?	Yes / No / Questionable
Are additional organisational / technical measures to be implemented:	Yes / No If yes, insert date and set reminder to secure an update
Free text box for additional comments:	
Has this DC reported similar breaches in the past?	Yes / No
Free text box for additional comment:	
Recommendation:	[Close, follow-up action or commence inquiry]
Rationale for recommendation:	
Taking into consideration all of the responses given to the questions on this form do you agree with risk rating of DC	Yes / No

Verification of Risk Assessment (GDPR)

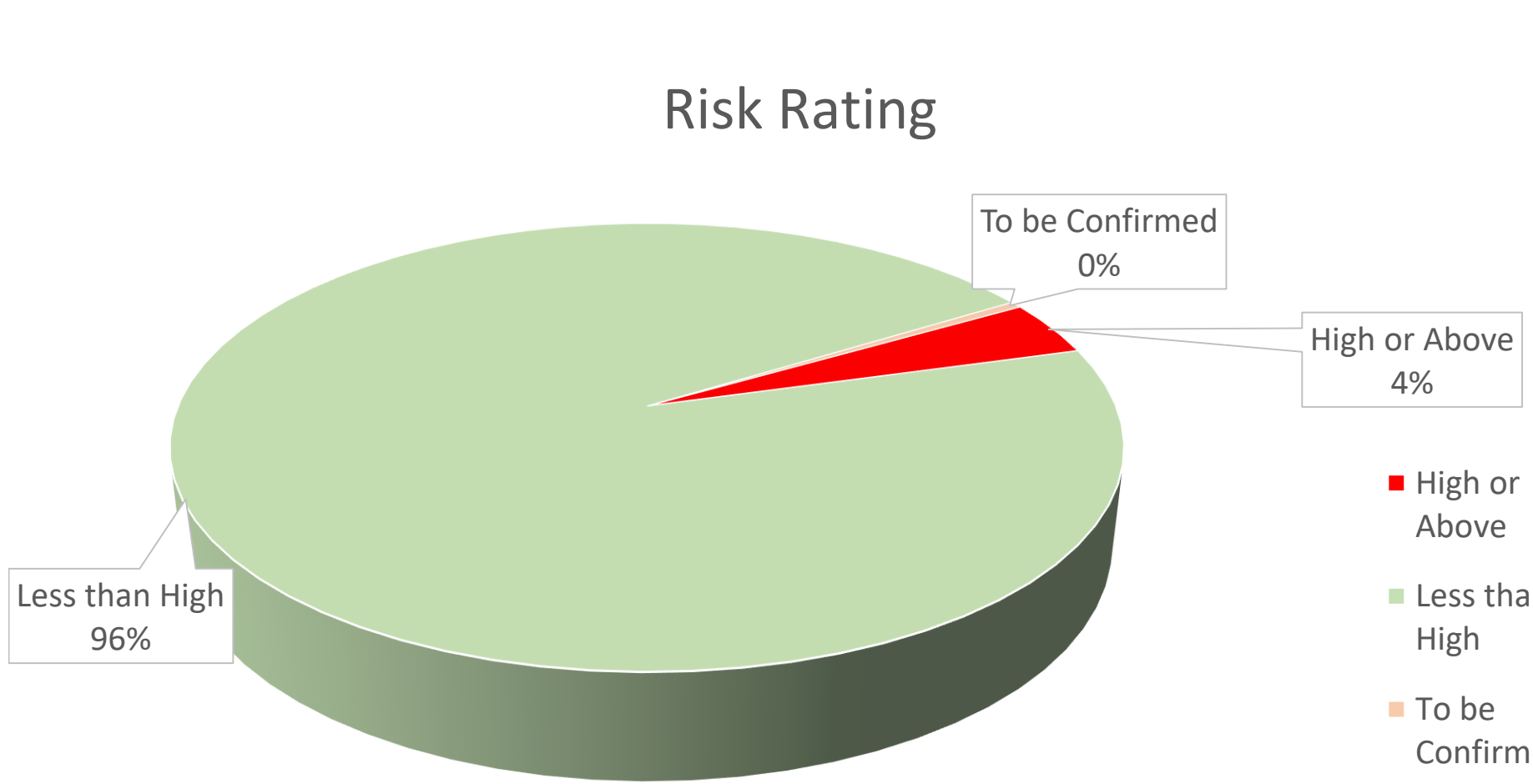
Quantitative Check list

- Applies weighting factors to volume, type of data to achieve a score
- Still requires Case Officer experience and knowledge
- Determines whether there is
  - No risk
  - Risk
  - High Risk

Risk Rating of GDPR Notified Breaches



Risk Rating of GDPR Notified Breaches



Case Studies

- **Highly sensitive data about sexual assault – postal delivery error**
- **Human error – wrong address on letter**
- **Loss of unencrypted USB key – health data**
- **Unauthorised disclosure of data to a journalist**
- **Financial Institution classed a mis-signed cheque as high risk**
- **Government body handling grant applications had webshell on server**
- **Creche sent personal financial data of employees and children's data to 32 individuals**
- **Consulting firm disclosed staff salaries to an employee**

Key Messages to controllers

In the event of a personal data breach:

- **Report on Time**
- **Contact data subjects without undue delay**
- **Clearly describe the issue, the steps taken and the planned steps**
- **Have a Breach Playbook and train your staff**
- **Retain your Logs, Record of Processing, Breach Records**