

It's not all fine(s)

Insights from data protection enforcement action (2018 – present)

SYNOPSIS: This hour-long session was led by the Bailiwick's Deputy Data Protection Commissioner Rachel Masterton. Rachel explored the key lessons that can be learned since data protection laws were strengthened in 2018. She explored key insights from local cases involving enforcement action. The session also covered what powers the local regulator (the ODPA) have, and how you might use this knowledge in your compliance work. These insights will help attendees navigate the evolving landscape of data protection.

Summary of enforcement powers available to ODPA

We want to engage with community via the principles of Balance, Trust, and Partnership.

- **Balance:** proportionate enforcement, awareness & learning vs. regulation, right tools & approach for the job.
- **Trust:** integrity, accountability, transparency, clear about what we are doing & why
- **Partnership:** domestic & global, sector regulators, other data protection authorities, stakeholders

If a [member of the public makes a formal complaint](#) about how their personal data has been handled, we can investigate it. Or we can launch an **inquiry** on our own initiative if we have concerns about an [organisation's compliance with the law](#).

Key enforcement powers:

- **'Determination'** – a formal finding that the activity under investigation has or will breach the law.
- **'Reprimand'** – a formal recognition that the law has been breached.
- **'Warning'** – a formal signal not to do something.
- **'Enforcement Order'** – an instruction compelling an organisation to take action to address shortcomings.
- **'Fine'** – a financial penalty issued in recognition of recklessness and/or harm caused by a specific breach.
- **'Information notice'** – a instruction which compels information, answers or documents to be provided.
- **'Audit'** – a formal check of whether an organisation has taken actions it was told to take.
- **'Public statement'** – a [statement to the media](#) about a particular matter that can be learned from and that an organisation is held to account for.

Our enforcement approach

- **Outcome based** – what can be done to put something right? What does the complainant want? What is proportionate? Systemic vs. one-off.
- **Learning** – internal, what can we do better, external, to improve practice, learn from others mistakes, guidance to address issues we are seeing commonly, sharing good & bad practice, sharing what we are doing.
- **Partnership** – we work with local organisations to ensure information is shared more broadly than we could on our own.

Key local case studies of enforcement action

1. **CCTV** – installed for crime prevention, recorded on phone by staff and circulated outside organisation. *Learning* – be clear about how data is to be used, make sure all staff know, restrict access to only those that need it.
2. **DSAR** – timescales – Data Subject Access Request made by an individual, extension applied but after 1 month response deadline, response not provided in the extra 2 months either. *Learning* – respond in time, have a process that works.

3. **Consent** – consent sought by recruitment agency, specifically only to reveal ID if individual agreed. CV was sent to a company with name in subject line of email, individual regularly dealt with that company.
Learning – use data only as you say you will, consent means consent.
4. **Mistracing** – firm helping client trace debtor used third party tracing agency, they provided an address in another jurisdiction, debt letter sent to new address, not the right person (but did know the person).
Learning – take care when sending things, if you are not sure, don't send sensitive stuff.

Lessons / trends

- **Enforcement action** trend moving from Reprimands more towards Orders, this is because of focus on outcome-focus.
- **Operative provisions breached** – [data protection principles](#) are breached often, timescales are also a big issue, '[right to information](#)' features a lot too as it's often because something unexpected has happened.
- **Self-reported breaches** – clear trend towards 'disclosure' of personal data being [the most reported incident](#). 'Access' issues are normally more cyber related, and feature strongly.

How to apply these in your compliance work

- Compliance is not just a once-a-year tickbox exercise, there needs to be [continual improvement](#).
- Think about how you can learn from others' mistakes.
- Know your data and how it is used, where are your risk points? How can you apply the lessons learned in your organisation.
- Make compliance an organisation-wide enterprise, get Board on side, make sure everyone knows [how to alert you to a breach](#) and [how to identify a data subject access request](#).

Looking ahead to interesting ongoing cases, technological development

- Ongoing local cases: system resilience and [direct marketing](#).
- International developments: [artificial intelligence](#) is under regulators' microscope. Dark patterns/deceptive design patterns – [GPEN privacy sweep](#) on this happened recently, locally we looked at gambling sites.

Help & advice

If you are responsible for personal data, we cannot do your job for you, but we can support you into making better decisions around your data handling practices.

- Visit our [information hub](#) for a range of resources for everyone including supporting guidance on understanding and complying with [your legal obligations](#).
- Explore recordings of our previous events/webinars, or access explainer videos [please visit our YouTube channel](#).
- Listen to some long-form insights and discussion on data protection issues [please explore our podcast series](#).
- Learn from statistics on types of personal data breaches reported locally [please visit our Reports & Statistics area](#).
- Receive monthly updates from us [please sign up to our newsletter](#).
- For frequent updates, [please follow us on LinkedIn](#).
- Talk something through with us, anonymously or otherwise, please do not hesitate to [contact us](#).
- Please come along to one of our regular, free [drop-in sessions](#), or if you want to explore something in more depth [please request a study visit](#), or [apply to enter our Sandbox](#).
- Explore [Project Bijou](#), a social initiative that goes beyond law and aims to engage people on a cultural level, to promote decision-making driven by ethics and human-values.