

# Cycle and Stride for Active Lives Leaders' project GDPR and data protection basics



# What's the story?

1. GDPR – what is it and why do I care?
2. What is personal data and sensitive personal data?
3. How do I know if I am holding this data?
4. **Exercise:** what data does my organisation hold?
5. I need that data to do my job! How can I stay legal?
6. Staying legal
7. Reporting breaches
8. What about information that appears on social media?
9. **Exercise:** what do I need to do to stay legal?
10. Summary and close

# Upfront disclaimer

This is not legal advice, we are not legally trained.

If you are concerned about the data you hold,  
get legal advice.

**GDPR**

**What is it and why do I care?**

# What is GDPR?

privacy

safety

GDPR is a good thing.

It establishes in law that **your data belongs to you, and you control who uses it, when and how.**



**But it can a big pain...**

**It means your org is responsible for looking after personal data you hold.**

**Even if the data is stolen by 'bad people' or leaked by suppliers like Microsoft, it's still your responsibility**

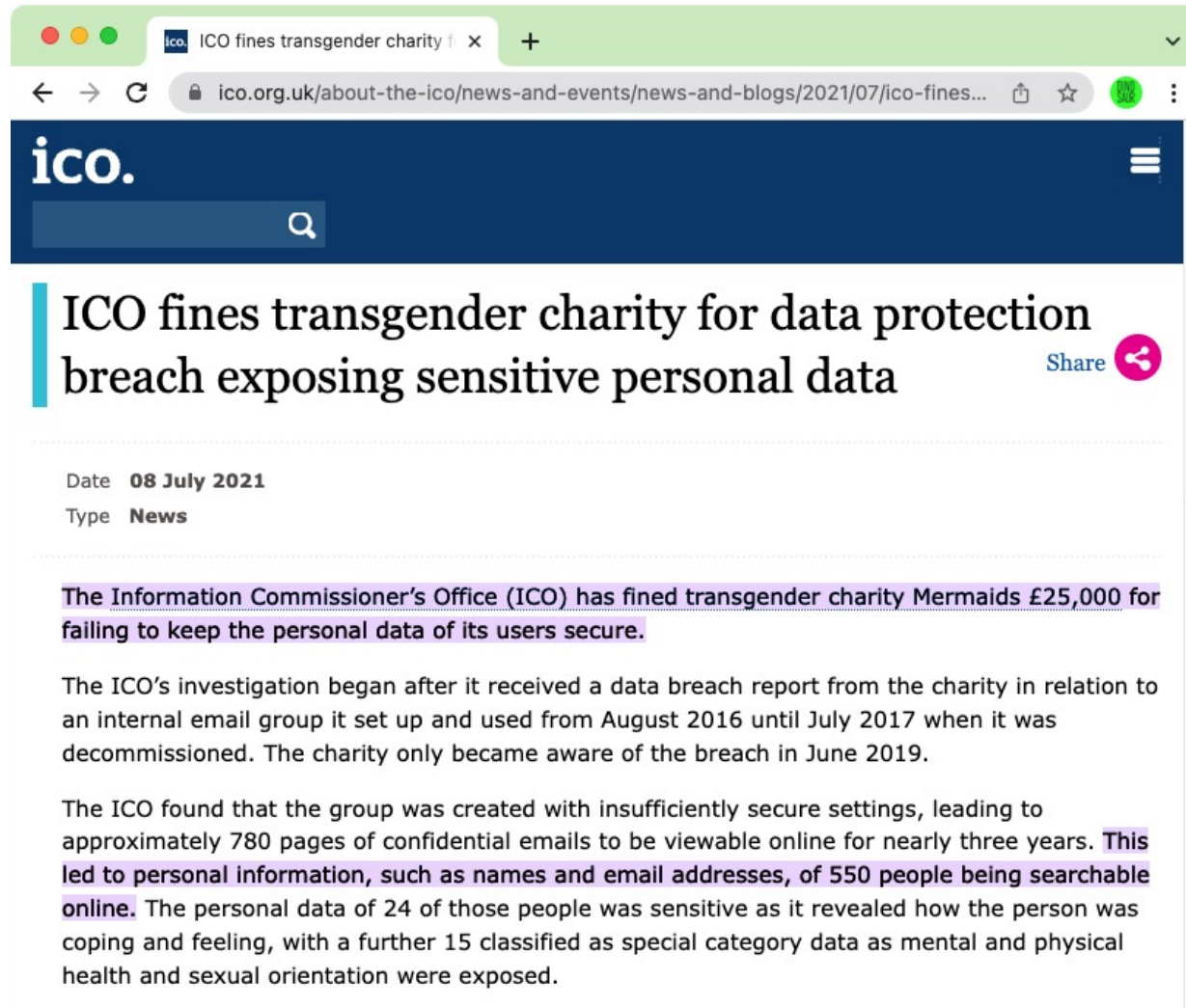


# What happens if we get it wrong?

The penalties can be severe.  
**Fines of up to €20m or 4% of turnover, whichever is the larger.**

The Google logo, consisting of the word "Google" in its signature multi-colored font.The British Airways logo, featuring the text "BRITISH AIRWAYS" in blue capital letters next to a stylized red and blue wing graphic.The Amazon logo, featuring the word "amazon" in a dark blue, lowercase sans-serif font with a curved orange arrow underneath it.

# And charities aren't exempt



The screenshot shows a web browser window with the URL `ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-fines...`. The page features the ICO logo and a search bar. The main headline is "ICO fines transgender charity for data protection breach exposing sensitive personal data". Below the headline, the date is "08 July 2021" and the type is "News". The article text states: "The Information Commissioner's Office (ICO) has fined transgender charity Mermaids £25,000 for failing to keep the personal data of its users secure." It further details that the ICO's investigation began after a data breach report from the charity in August 2016, which was decommissioned in July 2017. The charity became aware of the breach in June 2019. The ICO found that the group was created with insufficiently secure settings, leading to approximately 780 pages of confidential emails being viewable online for nearly three years. This led to personal information, such as names and email addresses, of 550 people being searchable online. The personal data of 24 of those people was sensitive as it revealed how the person was coping and feeling, with a further 15 classified as special category data as mental and physical health and sexual orientation were exposed.

ico. ICO fines transgender charity for data protection breach exposing sensitive personal data [Share](#)

Date **08 July 2021**  
Type **News**

**The Information Commissioner's Office (ICO) has fined transgender charity Mermaids £25,000 for failing to keep the personal data of its users secure.**

The ICO's investigation began after it received a data breach report from the charity in relation to an internal email group it set up and used from August 2016 until July 2017 when it was decommissioned. The charity only became aware of the breach in June 2019.

The ICO found that the group was created with insufficiently secure settings, leading to approximately 780 pages of confidential emails to be viewable online for nearly three years. **This led to personal information, such as names and email addresses, of 550 people being searchable online.** The personal data of 24 of those people was sensitive as it revealed how the person was coping and feeling, with a further 15 classified as special category data as mental and physical health and sexual orientation were exposed.



# Remember: it's not about you

For community leaders, data protection is much more about being able to do what you do without causing safeguarding issues for the people in your care.



## Example one

Paperwork was sent to children's birth parents without redacting the adoptive parents' names and address. When the data controller discovered the breach, they did not inform the adoptive parents, who later contacted the controller to advise that the birth parents had been to their address and had to be removed by the police. The adoptive parents and the children had to relocate.

## ICO advice

The controller should have notified the adoptive parents as soon as they discovered the breach, as this incident presents a high risk to their safety. The controller was aware that this address should have remained confidential. The main reason for notifying a data subject is so they can take steps to minimise the risks to themselves. For example, if the controller had notified the adoptive parents, they could have moved into alternative accommodation sooner or put additional safeguarding measures in place. This incident would also need to be reported to the ICO as the threshold for reporting is lower than notifying the people affected by the breach. The controller should also investigate the causes of this incident to ensure they understand how and why it occurred and put in place steps to prevent a similar incident occurring in the future.

# And now, having scared you...

**There are simple things you can do to make sure that you aren't put out of business by a data breach.**

Taking reasonable steps to comply with the law and having good procedures in place really reduces your exposure. Before we go into that, you need to understand a bit about personal data.

**What is it that you are being tasked with protecting?**

**What is personal data?**

# What is personal data?



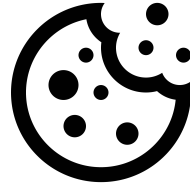
Name



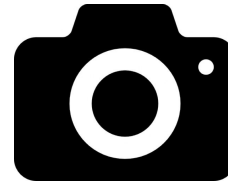
Device data



Email



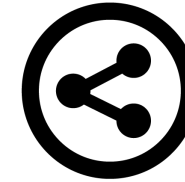
Cookie data



Photographs



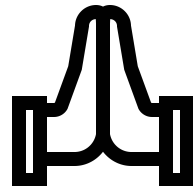
Address



Social



Biometrics



Religion



Tax & finance



Sexual prefs.



Political affiliation



Children's data



Health



Employment

Personal data is **anything** which can be used to identify a living person, even if only when combined with other data.

It's a **very** wide definition.

# Not all personal data is created equal

We're really concerned with a subset of this data.  
**Sensitive personal data.**

That's the stuff which could cause harm if it were leaked or made public.

So, what is that?

# Sensitive personal data



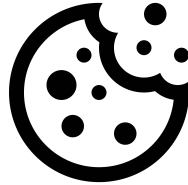
Name



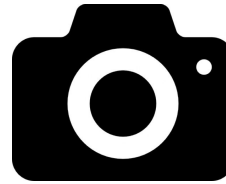
Device data



Email



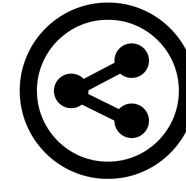
Cookie data



Photographs



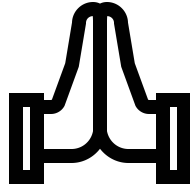
Address



Social



Biometrics



Religion



Tax & finance



Sexual prefs.



Political affiliation



Children's data



Health



Employment

Criminal or youth-justice related data should also be treated as sensitive. Mental health data is part of health data.

# Auditing your systems

You may need to do an audit of your people and systems to work out if you do hold this information, before you can decide what to do about it.

**So, let's look at that...**

**Exercise: What data does my organisation store?**



# How to do this

On a piece of paper, or a spreadsheet, or however you want to jot this down.

Really think about the corners of your systems and the kinds of information you gather to do your work.

Ask questions if you are unsure.

# What data might you hold?

- Non-sensitive data (name, address, phone number etc.)
- Date of birth is sometimes sensitive – treat it as such
- Religious affiliation and ethnicity
- Tax and finance
- Sex life and sexual preferences
- Political views or union affiliations
- Health data inc. mental health data
- Employment data – inc. CRB data
- Youth-justice or criminal data
- Copies of passport or other ID
- Anything else you can think of where it might be bad if it got out about.

# Where might you hold sensitive data?

- Social media
- Online chat – messaging platforms
- Email
- Billing and admin programs
- With suppliers (e.g. accountants, other community orgs, etc.)
- With staff
- Websites – not just yours – e.g. jotfrom
- Spreadsheets or member databases
- Old or lost phones and computers
- Backups
- ‘Informal’ data – notes, conversations

**Keep a note of what you’ve discovered, we’ll use it later.**

**I need this data to do my work!  
Do I have to delete it all?**

# That depends...

1. Are you allowed to hold the data?
2. Can people see, correct and control their data?
3. Will it be deleted when its no longer needed?
4. Is it securely held?
5. Do you have systems in place to:
  - a. Evaluate the risks of holding this data?
  - b. Manage who can access it?
6. A process for reporting data breaches?
7. Is it stored securely?

**Are you allowed to hold  
this data?**



# Are you allowed to hold this data?

## Consent is best.

Get people's **explicit opt-in** that they are OK with you holding data on them.

This should cover:

- What types of data you may hold
- Why you are holding it
- How they can access or delete it

# Getting consent 1/2

Consent should be recorded e.g. via a website registration form or on a paper sign-up.

This is just the same as getting insurance waivers or other consent for activities (e.g. insurance waivers for off-road cycling day or similar).

You may need to start doing this. Also, retroactively, to get that consent from people already signed-up.

Kids: Under the age of 13, you need parental consent.



# Getting consent 2/2

Consent must be ‘informed consent’.

People need to know what they are signing up to. You don’t need to give them your entire privacy policy on sign-up, a summary is fine as long as it tells them how to access it.

You can find a template privacy policy here:

<https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf>

This is a simple version, aimed at websites. If you aren’t using this on your website, simply omit the bit about cookies.

# What if I can't get consent?

It's not the only basis for holding data, just the best one. There are other reasons you can process data without explicit consent.

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

# What if I can't get consent?

Most of these are pretty clear, but legitimate consent can be slippery.

Only use it when:

- There's a limited privacy impact on the individual
- The individual should reasonably expect you to use their data in that way; **and**
- You cannot, or do not want to, bother them with disruptive consent requests when they are unlikely to object to the processing.

So, for example, you could use legitimate interest to avoid going back and obtaining consent from existing members as long as you **ONLY** hold non-sensitive information on them.

# Finally: you can anonymise data

You don't necessarily have to delete the data.

Anonymising it is also an option.

Just make sure there is no way for the person to be identified by the data.

# Where can I find out more?

If you are unsure about a particular example, use the information commissioner's office (ICO) interactive questionnaire to learn more:

<https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool>

A close-up photograph of a hand holding a white pipette tip. The tip is positioned over a small, white, cylindrical container. The background is a plain, light-colored surface. The text "Can people see, correct and control their data?" is overlaid in the center of the image.

**Can people see, correct  
and control their data?**

# Can people see, correct and control their data?

People have a right to see their data to make sure it is correct and legitimately held. Your privacy policy should contain clear instructions for how to get a copy of all data you hold on them. This is usually an email address to contact with Data Subject Access Requests (DSAR).

They can request it from anyone in your organisation. It doesn't have to go via this email address.

You are legally obliged to respond within 28 days. You can't usually charge for this, unless it's unreasonably expensive or onerous to comply.

# Can people see, correct and control their data?

Readability and portability:

You will have to supply this data in a format they can reasonably be expected to access – e.g. a PDF instead of a Word doc. A CSV instead of a database SQL dump.

Once received, they can normally request amendments, corrections or deletion – as long as there is no legal basis for you to keep the information (e.g. copies of an employment contract).



**Will it be deleted when  
it is no longer needed?**



# Data retention policy

Delete stuff when it's no longer needed.

Have a data retention policy, especially for sensitive information, that says how long different types of data will be kept for.

- Make sure it covers phones, Internet and messaging channels
- Make sure staff and volunteers understand it
- Make sure all computers and phones are completely wiped clean before being sold/donated on.

**Do you have the right  
processes in place?**



# Do you have processes in place?

In the event of a data-breach, you need to be able to show that you have:

1. Evaluated risk of holding this data with an impact assessment
2. Managed how data is stored, accessed, deleted and corrected
3. Trained staff and volunteers in data protection
4. Registered with the ICO as a data controller

# Impact assessment

This process shouldn't take long, but covers:

1. What data will you process?
2. Who else can access that data?
3. What bad stuff could happen if this data is breached?
4. How you store/process/delete data

You can find a template here:

<https://dinosauruk.sharepoint.com/:w:/g/Efur2uVQP8IAjlmwIHMWcr8B2EzbX-zPLGSsMJDeOI2sBw?e=xV7f6S>

## Privacy impact assessment form (PIA)

When you have identified that a PIA is necessary (by completing the PIA Screening forms), you should start to complete this document. You should start to complete this form at the beginning of the project planning stage, and before you have made any commitment to go ahead with the project. See Annex A for guidance on completing the PIA.

Project Name:	
PIA Completed by:	
Job Title:	
Date PIA Completed:	

### 1: Outline the Project & need for a PIA

Explain what the project involves, and the project aims. Summarise why the need for a PIA was identified.

For example:

The project involves [X] organisation sharing personal data about [X individuals] with Dinosaur. Dinosaur will also share personal data about [X individuals] with [X] organisation. The overarching purpose of the sharing is [XYZ]. The benefits of the share [to Dinosaur/the external organisation/the wider public etc] are [XYZ].

The relationship between Dinosaur and [X organisation] is (e.g. Dinosaur is providing contracted services to X organisation [or vice versa] and [explain the role each party is playing and their responsibilities e.g. x organisation is delivering an IT system or Dinosaur is providing advertising services].

The sharing of personal is due to take place [X project milestone] because [XYZ].

# Managed access to data

If the answer is no to any of these, you may need to put these measures in place.

Do you have a data retention policy?

You can find a template here:

<https://dinosauruk.sharepoint.com/:w:/g/Ede3Pyhv0AZKjtRbGoXJ4pQB-6HSNzFKqBcWbkQY0HFLbw?e=InHuXt>

Is it enforced? By whom?

You may need to appoint a data protection officer.

Do you have data management processes in place?

Is access to the data controlled? How? Is there an annual review of data held and routine removal of old data?

Are your staff and volunteers trained in data protection?

We use this course: <https://www.ihasco.co.uk/courses/detail/gdpr-training>

It costs about £30 a head. Other courses are available. We supplement that with training on our own company processes.

# Register with the ICO as a data controller



If you hold any sensitive data, you'll need to register with the Information Commissioner's Office (ICO). This is either free or cheap to not-for-profits.

You can do that here:

<https://ico.org.uk/for-organisations/data-protection-fee/register/>



**Do you have a process for  
managing data breaches?**



# Managing data breaches

You'll need to understand what should be reported and how that happens.

You'll also need to ensure that others in your organisation know to report possible data breaches, to whom, and how.

It's a good idea to have someone in the org who is responsible for this, especially for larger organisations.

**We'll go into this a bit more in a bit.**

[ DATA PROTECTION ]

Is data stored securely?



# Is your data stored securely?

## 1. Encrypt hard drives/memory

This is on by default in iOS and Android.

Easy to turn on in Macs: system preferences > Security and privacy > filevault Patchy implementation on PCs

Windows 11 machines – turn on ‘Bitlocker’

Older windows machines – same, but it may not work on cheaper machines.

## 2. Turn on password protection for devices if not already on

## 3. Only grant access to people who need it (and record who has access)


## 4. Avoid using USB sticks that are easily lost

## 5. Store information in the EU or UK

Including backups and email – usually available on paid-for email options, even paid gmail.

## 6. Make sure your website has a security cert

Indicated by a padlock just to the left of the address bar

 dinosaur.co.uk

# Reporting data breaches

# Report data breaches

**You have a legal duty to report within 72 hours of becoming aware of a data breach.**

To help you work out what/when to report, I'll go through:

- Identifying a data breach
- When and how to report it

# What is a data breach?



Losing a USB stick containing personal data



Lost/stolen computers and phones (even if protected/encrypted)



Accidentally sending personal data to the wrong person



Getting a virus (macs, droids and iPhones get malware too)



Social engineering 'blagger' attacks (e.g. email/phone phishing)



Server or network hacks

# Reporting

If you still aren't sure if you need to report a data breach, here's a handy guide.

In each case, take the worst possible bullet point.

E.g. if even a single person will suffer significant inconvenience or worse, then it's reportable.

## Appendix 2: Evaluation of Incident Severity

High Criticality: Major Incident	Contact:
<ul style="list-style-type: none"><li>Highly Confidential/Confidential Data</li><li>Personal data breach involves &gt; 1000 individuals</li><li>External <u>third party</u> data involved</li><li>Significant or irreversible consequences</li><li>Likely media coverage</li><li>Immediate response required regardless of whether it is contained or not</li><li>Requires significant response beyond normal operating procedures</li></ul>	<p><u>Lead Responsible Officer</u></p> <ul style="list-style-type: none"><li>To be determined by the Incident Management Team.</li></ul> <p><u>Other relevant contacts</u></p> <ul style="list-style-type: none"><li>Internal senior managers as required</li><li>Contact external parties as required i.e. police/ICO/client/individuals impacted</li></ul>
Moderate Criticality: Serious Incident	Contact:
<ul style="list-style-type: none"><li>Confidential Data</li><li>Not contained within Company</li><li>Breach involves personal data of more than 100 individuals</li><li>Significant inconvenience will be experienced by individuals impacted</li><li>Incident may not yet be contained</li><li>Incident does not require immediate response</li></ul>	<p><u>Lead Responsible officer</u></p> <ul style="list-style-type: none"><li>To be determined by the Incident Management Team.</li></ul> <p><u>Other relevant contacts:</u></p> <ul style="list-style-type: none"><li>Internal senior managers as required</li><li>Contact external parties as required i.e. police/ICO/client/individuals impacted</li></ul>
Low Criticality: Minor Incident	Contact:
<ul style="list-style-type: none"><li>Internal or Confidential Data</li><li>Small number of individuals involved</li><li>Risk to Dinosaur low</li><li>Inconvenience may be suffered by individuals impacted</li><li>Loss of data is contained/encrypted</li><li>Incident can be responded to during working hours</li></ul> <p><u>Example:</u> Email sent to wrong recipient with personal data attached. Loss of encrypted mobile device</p>	<p><u>Lead Responsible Officer</u></p> <ul style="list-style-type: none"><li>To be determined by the Incident Management Team.</li></ul> <p><u>Other relevant contacts:</u></p> <ul style="list-style-type: none"><li>Senior management, Head of Digital</li><li>Senior Management Team to follow up on policy procedures for managing personal data breaches</li></ul>

# Reporting - hygiene

**Don't just report your own data breaches.**

Even if it's a supplier who loses control of the data, you are still obliged to report. You aren't 'off the hook' just because someone else fouled up.

**You are still responsible for your customer's data.**



# Reporting

You can report breaches to the ICO here:

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/>

## **Don't just report to the ICO**

You will likely need to inform the people whose data has been breached outlining what data was involved and when it happened, so that they can act to protect themselves against the consequences.

**What about social media?**

# Social media

Social media is a special class of information.

You cannot be held responsible for the security of data that people have chosen to make public.

But, there are nuances.

- A closed Facebook group is considered public.
- A WhatsApp group is considered private.  
So, if you run a WhatsApp group, make sure you have a pinned post as a privacy notice and invite people via a link rather than by adding their phone number. Delete groups when no longer needed.
- Don't save information on public social to your own devices.  
If someone later takes down their post, they have chosen to remove it and it could be a grey area.

**Staying legal**

# What do we need to do to stay legal?

As before: that depends on what data you store.

So, we're going to explore that in an exercise...

**Exercise: What do I need to do to stay legal?**

# How to do this exercise

Refer back to the notes you made in the first exercise.

Now that you know how you need to handle sensitive data, take a look at the notes you made on what data you hold.

We'll help you decide on the best strategy to keep yourself legal and your members safe.

# How to do this exercise

For each type of sensitive data you hold, work out:

- Whether you absolutely need to **store** this info. to do what you do
- If there is a way you can work around collecting and storing this information e.g. by anonymising it.

Remember: if you store sensitive personal information, you will need to put in place data protection measures.



# Data management strategies

## 1. **Avoid: delete existing and don't collect**

We don't hold sensitive data or, now that I know what this is, I will delete or anonymise what I have, be mindful not to collect it in future and will train staff and volunteers in data protection

## 2. **Compliance: put data protection in place**

We will obtain consent for the sensitive data that we cannot avoid collecting and:

- a. Do a risk assessment on data you hold
- b. Put in place and enforce data retention policy
- c. Add data protection to basic training for volunteers
- d. Register with ICO
- e. Have someone in the org. whose job it is to monitor compliance on an annual basis

**And don't panic!**

# If the worst happens

If you do have sensible procedures in place, you may not even be fined for data breaches.

The big fines tend to be levied on organisations who made little or no effort to keep their data secure. Especially if they had the resources and money to do so. A small charity is unlikely to fall in that category.

***Any* questions?**

# Session feedback

Please take a minute or two to feedback on tonight's session.

<https://form.jotform.com/220413442620037>

A large crowd of people is seen from behind, many holding up their phones to take pictures. The air is filled with a thick, colorful mist of yellow, pink, and blue powder. A blue balloon is visible on the right side. The sky is bright blue with scattered white clouds. The overall atmosphere is festive and celebratory.

**Thank you!**