Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ◉ Initial report – report complete
- ○ Follow-up report – report complete
- ○ Initial report – additional information to follow
- ○ Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ◉ I consider the incident meets the threshold to report
- ○ I do not consider the incident meets the threshold to report, however I want you to be aware
- ○ I am unclear whether the incident meets the threshold to report

Size of organisation

- (•) Fewer than 250 staff
- ( ) 250 staff or more

Is this the first time you have contacted us about a breach since the GDPR came into force?

- ( ) Yes
- (•) No
- ( ) Unknown

About the breach

Please describe what happened

On October 1, 2023, a user by the name of Green-Prompt6762 posted on the unofficial 23andMe subreddit claiming to have breached 23andMe's systems, offering customer information for sale, and posting a sample of the alleged stolen data (the "Reddit Post").

Following the post, 23andMe immediately began investigating the incident and on October 5, 23andMe confirmed the incident was genuine.

On October 12, 2023, 23andMe identified the customers whose personal data was affected by the incident. The breach was limited to those customers who chose to make certain pesonal data available to other customers who were identified as 'DNA Relatives' (those other users with whom they share identical DNA segments).

Please describe how the incident occurred

23andMe's investigation is ongoing. At this time, it is uncertain when the threat actor was able to access certain 23andMe accounts in instances where customers employed identical usernames and passwords (login credentials) on other websites that were previously compromised that the customers used as login credentials for 23andMe.com.

How did the organisation discover the breach?

On being notified of the Reddit Post, October 1, 23andMe immediately began investigating the allegations in the Reddit Post to determine whether the claims were genuine.

What preventative measures did you have in place?

23andMe maintains a rigorous privacy and security program in accordance with ISO 27001, ISO 27701, and ISO 27018 standards: 23andMe employs a staff of white hat hackers to continuously test the security of the application and infrastructure. In addition, 23andMe maintains a public bug bounty programme where hundreds of researchers test and report security vulnerabilities for reward. 23andMe additionally engages with a third party to conduct, on an annual basis, penetration testing.

Was the breach caused by a cyber incident?

- (•) Yes
- ( ) No
- ( ) Don't know

When did the breach happen?

Date: Unknown Time:

When did you discover the breach?

Date: 5 October 2023 Time:

Categories of personal data included in the breach (tick all that apply)

- [x] Data revealing racial or ethnic origin
- [ ] Political opinions
- [ ] Religious or philosophical beliefs
- [ ] Trade union membership
- [ ] Sex life data
- [ ] Sexual orientation data
- [ ] Gender reassignment data
- [ ] Health data
- [x] Basic personal identifiers, eg name, contact details

☒ Identification data, eg usernames, passwords

☐ Economic and financial data, eg credit card numbers, bank details

☐ Official documents, eg driving licences

☒ Location data, eg coordinates

☐ Genetic or biometric data

☐ Criminal convictions, offences

☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

The threat actor downloaded certain accounts' unencrypted profile information which a customer creates and chooses to share with their genetic relatives in 23andMe's DNA Relatives feature. The types of information that 23andMe customers may choose to include in the profile they share with relatives via the DNA Relatives feature include the "DNA Relatives display name", how recently the customer logged into their account, relationship labels (masculine, feminine, neutral), predicted relationship and percentage of DNA shared with your matches, ancestry reports and matching DNA segments (optional), location (optional), ancestor birth locations and family names (optional), profile picture (optional), birth year (optional), link to Family Tree (optional)

As set out above, all information that 23andMe customers choose to share with their genetic relatives in 23andMe's DNA Relatives feature is optional except their display name, last login, relationship labels (predicted relationship labels (e.g., brother, sister, sibling)), and if a genetic match, then predicted relatedness.

Number of personal data records concerned?

1,103,647 total (18,856 located in the UK)

How many data subjects could be affected?

1,103,647 total (18,856 located in the UK)

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☒ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

There is no indication that any of the impacted 23andMe customers has had their rights or freedoms limited as a result of the incident.

There is no indication that any of the impacted 23andMe customers has been prevented from exercising control over their personal data by, for example, unauthorized password changes.

FOIA s.44 - Prohibition on disclosure [redacted]

Is the personal data breach likely to result in a high risk to data subjects?

- ○ Yes
- ◉ No
- ○ Not yet known

Please give details

See above

(Cyber incidents only) Recovery time

- (●) We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ( ) We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ( ) We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- ( ) We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- (●) Yes
- ( ) No
- ( ) Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

All employees are required to complete security and privacy trainings within 30 days of starting employment with 23andMe, and on an annual basis thereafter. This includes training on the following: security essentials, data security, General Data Protection Regulation and US Privacy laws. 23andMe requires completion of additional role-based security and privacy trainings.

(Initial reports only) If there has been a delay in reporting this breach, please explain why

On October 12, 23andMe first identified the customers whose DNA Relatives profile information had been downloaded by the threat actor. At that time, 23andMe immediately began determining 23andMe's breach notification obligations in the 56 countries where impacted customers are located.

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

On October 10, 2023, 23andMe sent emails to all customers advising of the incident and requiring customers to change their password, and encouraging customers to enable multi-factor authentication (MFA).

On October 13, 2023, 23andMe emailed the impacted customers advising that their profile information shared through the DNA Relatives feature had been accessed in the incident.

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

23andMe's investigation is ongoing. It has required all 23andMe customers to change their password and encouraged them to use multi-factor authentication, which 23andMe has offered since 2019. 23andMe has also temporarily paused certain functionality within the product as it investigates the incident.

Describe any further action you have taken, or propose to take, as a result of the breach

See above

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ◉ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ○ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- (•) Yes
- ( ) No
- ( ) Don't know

If you answered yes, please specify

23andMe will report the incident to data protection authorities in all territories where affected data subjects are located, or in some cases of which the data subejcts are citizens or residents and, to the extent required under applicable laws, 23andMe will report this incident to other public authorities.

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

- (•) Yes
- ( ) No

If yes:

Please confirm the Code/Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

- ○ Yes
- ○ No

Have you informed the relevant Monitoring Body or Certification Body?

- ○ Yes
- ○ No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

Report a suspicious website - NCSC.GOV.UK

About you

Organisation (data controller) name

23andMe, Inc.

Registration number

If not registered, please give exemption reason

The controller does not process personal data in the UK.

Business sector

Direct-to-Consumer Genetic Test

Registered organisation address

23andMe, Inc.

349 Oyster Point Blvd,

South San Francisco, CA 94080

USA

Person making this report

In case we need to contact you about this report

Name: [redacted] - Greenberg Traurig LLP

Email: [redacted]

Phone: [redacted]

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ○ Initial report – report complete
- ○ Follow-up report – report complete
- ○ Initial report – additional information to follow
- ◉ Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference: IC-264824-L0W2

Reason for report – after consulting the guidance

- ◉ I consider the incident meets the threshold to report
- ○ I do not consider the incident meets the threshold to report, however I want you to be aware
- ○ I am unclear whether the incident meets the threshold to report

Size of organisation

- ○ Fewer than 250 staff
- ◉ 250 staff or more

Is this the first time you have contacted us about a breach since the GDPR came into force?

- ○ Yes
- ○ No
- ◉ Unknown

About the breach

Please describe what happened

Following the report made and given ICO case reference IC-264824-L0W2 on 15 October 2023, 23andMe became aware that on October 17, 2023, a user with the name Golem, posted data which he claimed was from 23andMe, calling it the "Great Britain - Originated 4M Genetic Dataset" on the cybercrime forum known as BreachForums website (https://breachforums.is). On October 18, 2023, the same user posted additional information on BreachForums which he claimed was downloaded from 23andMe and included data about individuals with German ancestry. 23andMe immediately began investigating to determine whether the claims and the data were genuine.

By October 23, 23andMe had verified the data was genuine and had identified the customers whose DNA Relatives profile information had been downloaded and posted to download on the BreachForums website. As part of the investigation, 23andMe also independently determined additional customers who had their DNA Relatives profile information downloaded, but had not been posted on the BreachForums website. At that time, 23andMe immediately began determining 23andMe's breach notification obligations in the 62 jurisdictions where impacted customers are located.

Please describe how the incident occurred

While 23andMe's investigation is ongoing, at this time, as described in the previous incident report, it appears that the threat actor was able to access certain 23andMe accounts in instances where 23andMe users employed

identical usernames and passwords (login credentials) on other companies' websites, that were previously compromised, that the users used as login credentials for 23andMe.com.

How did the organisation discover the breach?

See above

What preventative measures did you have in place?

23andMe maintains a rigorous privacy and security program in accordance with ISO 27001, ISO 27701, and ISO 27018 standards: 23andMe employs a staff of white hat hackers to continuously test the security of the application and infrastructure. In addition, 23andMe maintains a public bug bounty programme where hundreds of researchers test and report security vulnerabilities for reward. 23andMe additionally engages with a third party to conduct, on an annual basis, penetration testing.

Was the breach caused by a cyber incident?

- (•) Yes
- ( ) No
- ( ) Don't know

When did the breach happen?

Date: Unknown Time:

When did you discover the breach?

Date: 24 October 2023 Time: 07:59

Categories of personal data included in the breach (tick all that apply)

- [x] Data revealing racial or ethnic origin
- [ ] Political opinions
- [ ] Religious or philosophical beliefs
- [ ] Trade union membership
- [ ] Sex life data
- [ ] Sexual orientation data

☐ Gender reassignment data

☐ Health data

☒ Basic personal identifiers, eg name, contact details

☒ Identification data, eg usernames, passwords

☐ Economic and financial data, eg credit card numbers, bank details

☐ Official documents, eg driving licences

☒ Location data, eg coordinates

☐ Genetic or biometric data

☐ Criminal convictions, offences

☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

The threat actor downloaded certain accounts' unencrypted profile information which a customer creates and chooses to share with their genetic relatives in 23andMe's DNA Relatives feature. The types of information that 23andMe customers may choose to include in the profile they share with relatives via the DNA Relatives feature include the "DNA Relatives display name", how recently the customer logged into their account, relationship labels (masculine, feminine, neutral), predicted relationship and percentage of DNA shared with your matches, ancestry reports and matching DNA segments (optional), location (optional), ancestor birth locations and family names (optional), profile picture (optional), birth year (optional), link to Family Tree (optional)

As set out above, all information that 23andMe customers choose to share with their genetic relatives in 23andMe's DNA Relatives feature is optional except their display name, last login, relationship labels (predicted relationship labels (e.g., brother, sister, sibling)), and if a genetic match, then predicted relatedness.

Number of personal data records concerned?

5,621,179 total (including 1,103,647 already reported);

77,412 located in the UK including the already reported)

How many data subjects could be affected?

As above

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☒ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

There is no indication that any of the impacted 23andMe customers has had their rights or freedoms limited as a result of the incident.

There is no indication that any of the impacted 23andMe customers has been prevented from exercising control over their personal data by, for example, unauthorized password changes.

FOIA s.44 - Prohibition on disclosure [redacted]

Is the personal data breach likely to result in a high risk to data subjects?

- ○ Yes
- ◉ No
- ○ Not yet known

Please give details

See above re detriment

(Cyber incidents only) Recovery time

- (•) We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ( ) We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ( ) We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- ( ) We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- (•) Yes
- ( ) No
- ( ) Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

All employees are required to complete security and privacy trainings within 30 days of starting employment with 23andMe, and on an annual basis thereafter. This includes training on the following: security essentials, data security, General Data Protection Regulation and US Privacy laws. 23andMe requires completion of additional role-based security and privacy trainings.

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

On October 10, 2023, 23andMe sent emails to all customers advising of the incident and requiring customers to change their password, and encouraging customers to enable multi-factor authentication (MFA).

As part of the ongoing security investigation, on October 20, 2023, 23andMe temporarily disabled some features within the DNA Relatives tool as an additional precaution to protect the privacy of our customers.

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Beginning October 23 and concluding on October 24, 23andMe emailed the impacted individuals advising that their profile information, which they chose to share through 23andMe's DNA Relatives feature, had been accessed in the incident.

23andMe's investigation is ongoing. It has required all 23andMe customers to change their password and encouraged them to use multi-factor authentication, which 23andMe has offered since 2019. 23andMe has also temporarily paused certain functionality within the product as it investigates the incident.

Describe any further action you have taken, or propose to take, as a result of the breach

See above

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ◉ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ○ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- (●) Yes
- ( ) No
- ( ) Don’t know

If you answered yes, please specify

23andMe will report the incident to data protection authorities in all territories where affected data subjects are located, or in some cases of which the data subejcts are citizens or residents and, to the extent required under applicable laws, 23andMe will report this incident to other public authorities.

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

- ( ) Yes
- (●) No

If yes:

Please confirm the Code/Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

- ○ Yes
- ○ No

Have you informed the relevant Monitoring Body or Certification Body?

- ○ Yes
- ○ No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

Report a suspicious website - NCSC.GOV.UK

About you

Organisation (data controller) name

23andMe, Inc.

Registration number

If not registered, please give exemption reason

The controller does not process personal data in the UK.

Business sector

Direct-to-Consumer Genetic Test

Registered organisation address

23andMe, Inc.

349 Oyster Point Blvd,

South San Francisco, CA 94080

USA

Person making this report

In case we need to contact you about this report

Name: [redacted] - Greenberg Traurig LLP

Email: [redacted]

Phone: [redacted]

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

Email

RE: ICO Case Reference: I...

Regarding | Worked By | Status Reason | R...
Activity Marker | E... Direction | I...

Email

From	[redacted]
To	ICO Casework
Cc	[redacted]
Subject	RE: ICO Case Reference: IC-264824-L0W2
Display Name	
Date Received	11/11/2023 00:42
Email Address	[redacted]

External: This email originated outside the ICO.

Dear Mr. Dodd,

We write in response to your email below seeking further information about the breach reports that 23andMe, Inc. submitted in October.

While 23andMe's investigation of the October incident is ongoing, at this time we believe the threat actor was able to access numerous 23andMe accounts in instances where 23andMe customers employed identical usernames and passwords (login credentials) on other companies' websites that were previously breached. 23andMe believes that after gaining access to such accounts, the unauthorized third party downloaded files that included the data points that certain customers, who chose to participate in 23andMe's DNA Relatives feature profiles, decided to share with their genetic relatives. The third party then created posts regarding the stolen data, with links to download files that contained theses data points for various individuals on the reddit.com and breachforums.is sites as set out in the two initial reports to the ICO. It is unclear who may have downloaded the information posted; however, we have identified other websites where links to some of the files posted by this user are reposted. 23andMe has successfully had several of these re-postings removed from these other websites, and is working to get the other links removed. The incident did not involve an availability breach, and no data was lost, corrupted or otherwise required restoration.

As noted above, the information downloaded by the threat actor included data that 23andMe customers decided to include in the profile that they share with relatives via the DNA Relatives feature are described at https://customercare.23andme.com/hc/en-us/articles/18262768896023 and set out below. All information that 23andMe customers choose to share with their genetic relatives in 23andMe's DNA Relatives feature is optional except their display name, last login, relationship labels, and if a genetic match, then predicted relatedness. The types of personal data about an impacted individual that may have been include in the information downloaded by the threat actor includes:

- **DNA Relatives display name**
- **How recently the individual logged into their account**
- **Relationship labels (masculine, feminine, neutral)**

- Predicted relationship and percentage of DNA shared with matches
- Ancestry reports and matching DNA segments (optional)
- Self-reported location (optional)
- Ancestor birth locations and family names (optional)
- Profile picture (optional)
- Birth year (optional)
- A link to their Family Tree (optional)
- Anything they have added to the "Introduce yourself!" section (optional)

As of the date of this email we are unaware of any evidence of detriment to any impacted data subject other than a loss of confidentiality in respect of the data concerned, noting that the personal data concerned were data that the data subjects had chosen to share with other users of the 23andMe site with whom the data subjects had no prior contact or knowledge, albeit on a more limited basis.

Please let us know if you have any further questions.

Sincerely,

FOIA s.40(2) - Personal data that doesn't fall under s.40
Shareholder

Greenberg Traurig, LLP
101 2nd Street | Suite 2200 | San Francisco, CA 94105-3668
FOIA s.40(2) - Personal data that doesn't fall | www.gtlaw.com | View GT Biography

Albany. Amsterdam. Atlanta. Austin. Boston. Berlin*. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Las Vegas. London*. Long Island. Los Angeles. Mexico City*. Miami. Milan*. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. Seoul*. Shanghai. Silicon Valley. Singapore*. Tallahassee. Tampa. Tel Aviv*. Tokyo*. Warsaw*. Washington, D.C. West Palm Beach. Westchester County.

*Berlin: Greenberg Traurig's Berlin Office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP.; London: Operates as a separate UK registered legal entity; Mexico City: Operates as Greenberg Traurig, S.C.; Milan: Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP; Seoul: Operated by Greenberg Traurig LLP Foreign Legal Consultant Office; Singapore: Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore; Tel Aviv: A branch of Greenberg Traurig, P.A., Florida, USA; Tokyo: Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP; Warsaw: Operates as GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k.

From: icocasework <icocasework@ico.org.uk>
Sent: Friday, November 3, 2023 9:33 AM
To: FOIA s.40(2) - Personal data that doesn't fall under s.40(1)
Subject: ICO Case Reference: IC-264824-L0W2

EXTERNAL TO GT

3 November 2023

Case Reference: IC-264824-L0W2

To whom it may concern,
I am a Lead Technical Investigations Officer for the Information Commissioner's Office (ICO), and I have been assigned the breach report you submitted on behalf of your organisation for investigation.

This case has been considered under the General Data Protection Regulations (GDPR) due to the nature of the processing involved, and that the incident occurred on or after 25 May 2018.

Thank you for your breach report submission, I now require some further information, please therefore provide responses to the below:

1. **How did the incident occur?**
2. **What was the initial point of entry?**
3. **How many UK Data Subjects have been affected?**
4. **Is there any evidence of data exfiltration?**
5. **What is the nature of the affected data?**
6. **Have you recovered your systems and restored your data? Confirm how and when (i.e. data recovered from off site back ups);**
7. **Is there any evidence of detriment?**

Please provide the above information as soon as possible, and no later than 10 November 2023.

Thank you for your co-operation and assistance during our investigation into this matter.

Kindest Regards,

Elliot Dodd
Lead Case Officer
Information Commissioner's Office

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6486 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice**.**

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at postmaster@gtlaw.com, and do not use or disseminate the information.

ATTACHMENTS

File Name	Followed	File Size (Byte...
image001.png	No	6,018

1 - 1 of 1 (0 selected) Page 1