

Bolton at Home Ltd,  
98 Waters Meeting Road  
Bolton  
BL1 8SW

By email only to: [REDACTED]

7 June 2022

[REDACTED],

**Case Reference Number INV/0561/2021**

I write to inform you that the ICO has now completed its investigation into the inappropriate disclosure of personal data.

In summary, it is my understanding that a staff member from Starts With You (SWY – a Bolton at Home subsidiary company) left a message on a telephone number provided on the data subject's record. The number was actually the telephone number of the data subject's husband, who she was intending to leave. This information had been provided to SWY by Bolton at Home (BH). The message contained details of the new address that the data subject was intending to move to.

This case has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) due to the nature of the processing involved.

For more information about our powers under the data protection legislation please see the attached leaflet.

- ICO Enforcement leaflet - GDPR and DPA 2018

**Our consideration of this case**

We have investigated whether BH has complied with the requirements of data protection legislation.

In the course of the investigation we have noted that:

- The data subject approached BH for alternative accommodation due to alleged domestic abuse. The detriment caused to the data subject by the inappropriate disclosure of her personal data is therefore significant.
- The data subject and her husband (the reported abuser) were both already registered with BH. The data subject applied for the new property in her name only and specified that she was moving due to domestic violence and her husband did not know she was leaving him. When she requested alternative accommodation, a separate record was created by BH for the data subject, with her new address. Other details were copied over from the shared record that the data subject had with her husband, this included the husband's telephone number. There was no distinction on the new record as to who's number was who's.
- The data was provided to SWY by BH. The information was provided in a spreadsheet. The information relating to the data subject's situation was held on a different BH system, (known as ECCO) which only certain BH staff members had access to.
- On 1 March 2021, a staff member from SWY called both telephone numbers on the record in relation to offering an energy advice service. The staff member left a message on both numbers. By leaving the message on the data subject's husband's number he was made aware that the data subject was seeking alternative accommodation. He also became aware of where she was intending to move to.
- On 16 March 2021, the data subject complained to BH about the breach, explaining that her husband was now aware of her plans to leave and her new address. The disclosure had also resulted in the husband visiting the new address.
- Reporting the breach to the ICO was delayed. It took nine days, from BH being made aware of the breach on 16 March, to reporting the breach to the ICO on 25 March 2021. The staff member who took the complaint handled it solely as a service complaint.
- Discussion was then had between staff members as to whether it constituted a data breach or not. This delayed internal reporting. BH's

Information Governance Team was not made aware of the breach. While BH had a data breach policy in place, which covers reporting a breach, it was not correctly applied.

- The new record for the data subject was created by copying over information from the previous record, rather than starting afresh. This meant that chances to input correct and accurate data was missed.
- There were no markers copied over to the information provided to SWY regarding the alleged domestic violence, or that the husband should not be contacted.
- There were no markers on the new record denoting who's number was who's it was simply listed as 'home' and 'mobile'.
- At the time of the breach, there was no formal record creation policy or process in place for staff to follow.
- The informal warning code policy that was in use by a number of BH staff was only in draft form and not fully embedded in BH's processes.

We have also noted that:

- Staff uptake on data protection training appears to be low. The staff member involved in the breach was overdue their data protection training at the time of the breach.
- At the time of the breach, BH employed seven separate systems to handle various aspects of customer data. Personal data was not kept up to date across all of these systems and increased the likelihood of a breach of this nature occurring.

We have also considered and welcome the remedial steps taken by BH in light of this incident.

- BH states that it is working through its records to ensure data accuracy is thorough and that a system is in place to alert frontline staff (for example customer contact) to safeguarding markers when dealing with contact relating to a tenant record.

- The data subject and her son have now been accommodated in the property. Extra security measures have been taken and a domestic abuse marker has been placed on the property. BH kept in touch with the data subject to check that she was safe.
- All BH staff involved in the tenancy application were made aware of the data subject's situation.
- The husband's phone number has been removed from the record.
- BH state that 'toolbox talks' have been planned for all staff on data breaches. BH hopes that this will help staff identify breaches and understand the reporting process.
- The staff member involved in the incident has received her data protection refresher training, since the breach.
- BH has undergone a tender process to implement an integrated housing and asset management system to then retire old applications, due to be implemented in October 2022. This should mean less record systems to keep updated.

However, after careful consideration and based on the information provided, we have decided to issue BH with a reprimand in accordance with Article 58 of the UK GDPR.

### **Details of reprimand**

The reprimand has been issued in respect of the following processing operations that have infringed the UK GDPR:

- **Article 5(1)(d) – Accuracy**  
The UK GDPR requires a data controller to ensure that the personal data it processes remains accurate and up to date in line with the purposes for which it is being processed. In this case, a new record was created for the data subject by BH which included her husband's telephone number from a previous record in error. BH has provided no evidence of any policy, written procedure or guidance in place at the time of the breach which set out how

new records should be created. The lack of measures to prevent an inaccurate record being created in this case infringed Article 5(1)(d).

- **Article 5(1)(f) – Security**

The UK GDPR requires data controllers to process personal data securely by means of appropriate technical and organisational measures. Inaccurate data had already been included in the data subject's new record. A further chance to prevent the inappropriate disclosure of her new address was missed in that a warning code relating to alleged domestic abuse was not applied correctly to her record or the information shared in the spreadsheet with SWY. BH has confirmed that the informal warning code policy was in draft form only. The lack of a formal process in place was a failing and infringed Article 5(1)(f).

- **Article 33(1) – notification to supervisory authority**

The UK GDPR requires data controllers to notify the ICO of a personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it..." In this case, BH's internal reporting mechanisms failed which resulted in notification being made to the ICO outside the statutory time frame and an infringement of Article 33(1).

### **Further Action Recommended**

The Commissioner recommends that BH could take certain steps to improve compliance with the UK GDPR. In particular:

1. Consider implementing a record creation policy and process
2. Formalise the draft warning code policy and process
3. Ensure the above policies and processes are embedded within your data protection practices
4. Review your internal breach reporting policies and processes and make improvements where necessary to ensure future compliance with your article 33 obligations
5. Ensure adequate training is given to all staff on the above policies and processes

Please provide an update with regards to your progress on the above steps within the next six months and no later than 7 December 2022.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

<https://ico.org.uk/for-organisations/guide-to-data-protection/>

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:



[https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico\\_enforcement\\_communications\\_policy.pdf](https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf)

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the case closed.

Yours sincerely

  
Lead Case Officer – Civil Investigations  
Regulatory Supervision Service  
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow,  
Cheshire SK9 5AF  


*Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with,*

*including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website ([www.ico.org.uk](http://www.ico.org.uk)).*

*The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link (<https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/>).*

*We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.*

*If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk) .*

*Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.*

*For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)*