

Power Leisure Bookmakers Limited
Chancellors Road
London
W6 9HP

By email only to: [REDACTED]

6 December 2022

Dear [REDACTED]

Case Reference Number INV/0774/2021
Case Reference Number INV/0184/2022

We write to inform you that the ICO has now completed its investigation into Power Leisure Bookmakers Ltd (PLB). This investigation has considered the breaches reported to the ICO on 27 August 2021, 3 September 2021, 9 June 2022, and 7 July 2022.

[REDACTED]

[REDACTED]

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

Our consideration of this case

We have investigated whether PLB has complied with the requirements of the data protection legislation, by implementing appropriate technical and organisational measures, to ensure appropriate security of the personal data, affected by this breach.

Key Compliance Issues

Details of the particular failings by the PLB, are outlined below as follows:

1. PLB has failed to implement a robust security procedure to protect personal data, in direct contravention of Article 5(1)(f), which requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

[REDACTED]

[REDACTED]

2. The "flaw" in the security process also demonstrates a contravention of Article 24(1), whereby PLB has failed to implement appropriate technical and organisational measures and has failed to review and update measures as necessary.
3. Article 32(1) requires organisations to have a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

If this process had been adequately carried out, the "flaw" should have been identified earlier and should have been addressed by PLB.

4. PLB has failed to assess the appropriate level of security required, taking into account the risks from accidental loss or unauthorised disclosure of personal data, in direct contravention of Article 32(2).

[REDACTED]

5. Whilst the "flaw" in the original security process has been identified, many of the incidents also occurred as a result of staff not following the security process

[REDACTED]

[REDACTED]

6. PLB has confirmed that 95% of staff have completed data protection training within the last 12 months, and all [REDACTED] involved in these breaches had completed their training. However, despite this, the [REDACTED] involved in these breaches had had more than one 0% fail – this indicates a training/guidance issue within the organisation, whereby staff do not understand the implications of not adhering to procedures, or the data protection ramifications as a result.

[REDACTED]

Investigation Outcome

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

Details of reprimand

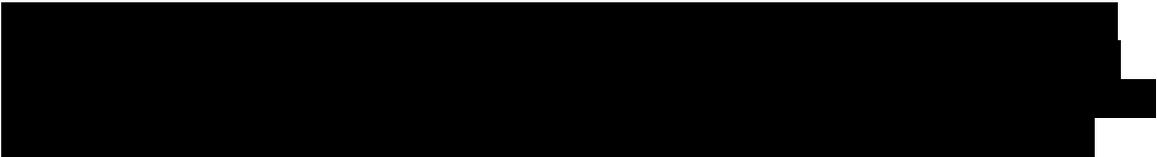
The reprimand has been issued in respect of the following processing operations that have infringed the UK GDPR:

- **Article 5(1)(f)** which states that “personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”
- **Article 24(1)** which states that “taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

- **Article 32(1)** which states that “taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) The pseudonymisation and encryption of personal data;
 - (b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”
- **Article 32(2)** which states that “in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”

Further Action Recommended

Alongside the ICO’s decision to issue PLB with a reprimand in this case, the Commissioner also considers that PLB should take certain steps to improve its compliance with the UK GDPR. In particular, we recommend that PLB should take the following steps:

1. Decide on a long-term solution, and implement a new security process, which you are satisfied ensures appropriate security of the personal data – reducing the risk of repeat incidents in future.
2. 
3. Take steps to test the integrity of any new processes introduced; particularly in those areas where data breaches have occurred.

4. Once a new security process is implemented, ensure all relevant staff are made aware of any changes to processes, by effectively communicating to and providing clear guidance to staff.
5. Ensure that the data protection policies/procedures/guidance of the organisation are complied with, by regular assurance testing and auditing. It is also advisable to test assurance of employee understanding of data protection matters from time to time; particularly in areas which are identified as high risk, due to the nature of personal data that is processed in those areas.
6. Review all internal security procedures on a regular basis to identify any additional preventative measures that can be implemented.
7. Consider including specific PLB breach examples, to training materials. This will assist staff in understanding how data protection relates specifically to their role.
8. Ensure staff are provided with sufficient data protection training for their roles and duties in the workplace. This can be achieved by reviewing the content and frequency of data protection training, and ensuring that sufficient practical guidance is given to staff in how to comply with the legislation. This training should also be tailored to specific roles, as levels of access to personal data may vary from person to person.
9. Consider sending more frequent reminders/conducting sessions more frequently with staff members, in relation to the importance of handling personal data securely and appropriately; along with the possible adverse effects of failing to adhere to established procedures.
10. Regularly review the guidance that is available on the ICO website.
11. Ensure that any future incidents reported to senior members of staff and the ICO are done so within 72 hours, to comply with the UK GDPR.

For completeness, we ask that PLB provides a progress update to the ICO on the above recommendations in six months' time, or by no later than **6 June 2023**. Unless otherwise instructed, please provide this update to [REDACTED]

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 UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

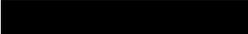
https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

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 matter closed.

Yours sincerely,

Alice Arnott
Investigation Officer - Civil Investigations
Regulatory Supervision Service
The Information Commissioner's Office


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).

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



Information Commissioner's Office

(<https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-datasets/>).

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 .

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