



ZWIĄZEK HARCERSTWA POLSKIEGO

ZARZĄD OKRĘGU w WIELKIEJ BRYTANII

POLISH SCOUTING ASSOCIATION (UK Region) Ltd.

Registered in England and Wales No.: 08352009,
Registered Charity England and Wales: 1155288, Scotland: SC045348
Registered Office: 23-31 Beavor Lane, London W6 9AR
Email: admin@zhpwb.org.uk



Polityka Postępowania w Przypadku Naruszenia Danych Osobowych

Podsumowanie dla Komendantów, Drużynowych i Instruktorów

Niniejszy dokument stanowi część systemu zarządzania Polish Scouting Association (UK Region) (znanego jako PSA UK Region) i zapewnia pełną zgodność z brytyjskim rozporządzeniem o ochronie danych osobowych 2018 (UK GDPR 2018) oraz ustawą o ochronie danych z 2018 roku (Data Protection Act 2018). Jako zarejestrowany w Wielkiej Brytanii podmiot prawny oraz formalny Administrator Danych (Data Controller), PSA UK Region ma prawny obowiązek stosowania odpowiednich środków organizacyjnych w celu ochrony danych i przestrzegania praw do prywatności. Wszyscy instruktorzy, drużynowi i wolontariusze są zobowiązani do przestrzegania tych ustawowych standardów.

Ten dokument wyjaśnia, czym dokładnie jest naruszenie danych osobowych (wyciek danych/data breach) oraz krok po kroku instrukcje, jak to zgłosić, jeśli coś pójdzie nie tak. Prawo brytyjskie nakłada bardzo surowe terminy zgłaszania takich zdarzeń. Umiejętność szybkiego rozpoznania wycieku i natychmiastowego powiadomienia Zarządu PSA UK Region jest obowiązkowa dla wszystkich instruktorów/ów, drużynowych i wolontariuszy.

Czym jest Naruszenie Danych Osobowych?

Naruszenie danych następuje wtedy, gdy informacje będące w posiadaniu kogoś z PSA UK Region zostaną przypadkowo lub bezprawnie zgubione, zniszczone, zmienione, ujawnione lub udostępnione nieupoważnionej osobie. Dotyczy to w równym stopniu dokumentów papierowych, jak i plików cyfrowych.

Naruszenie danych to nie tylko zgubienie lub wyciek informacji. To także sytuacja, w której dane stają się całkowicie niedostępne. Na przykład: jeśli awaria systemu, atak hakerski lub utrata dostępu zablokuje Ci konto Google Drive w PSA UK Region i podczas obozu nie będziesz mieć wglądu do kart zdrowia, według brytyjskiego prawa jest to oficjalnie naruszenie bezpieczeństwa danych.

Dwa Przykłady z Harcerstwa – Jakie Wyciągamy Wnioski?

Przykład 1: Ujawnienie poufnego adresu (Wysokie Ryzyko)

- Co się stało:** Drużynowy zuchów wysłał zgłoszenie na obóz do ojca zucha z prośbą o brakujący podpis. Drużynowy zapomniał zasłonić nowy adres zamieszkania matki dziecka. Matka wcześniej wyraźnie prosiła PSA UK Region, aby ze względów bezpieczeństwa nie udostępniać jej nowego adresu byłemu partnerowi. Drużynowy nie poinformował matki o swoim błędzie.
- Konsekwencje:** Ponieważ matka nie została ostrzeżona, nie mogła podjąć środków ostrożności. Ojciec pojawił się pod jej nowym domem, musiała interweniować policja, a matka z dzieckiem musieli się przeprowadzić.
- Wnioski:** Było to poważne naruszenie, które stworzyło bezpośrednie zagrożenie dla zdrowia i życia. Drużynowy powinien był natychmiast powiadomić Zarząd PSA UK Region oraz matkę, aby zdążyła się zabezpieczyć. Jako formalny Administrator Danych (Data Controller), PSA UK Region miał prawny obowiązek zgłosić ten przypadek do brytyjskiego urzędu ds. ochrony danych (ICO).

Przykład 2: Pomyłkowy e-mail do innego instruktora (Niskie Ryzyko)

- Co się stało:** Hufcowy chciał napisać do Komendanta Chorągwi Harcerzy w sprawie rodziny znajdującej się w trudnej sytuacji finansowej i zdrowotnej, prosząc o zniżkę na wyjazd na zlot. Przez pomyłkę wysłał e-mail do Komendantki Chorągwi Harcererek.
- Konsekwencje:** Komendantka Harcererek natychmiast usunęła tę wiadomość i poinformowała nadawcę o pomyłce. Ponieważ oboje instruktorzy działają wewnątrz PSA UK Region, przechodzą szkolenia z ochrony danych i zareagowali prawidłowo, nie było realnego zagrożenia dla rodziny.

- **Wnioski:** Tego zdarzenia nie trzeba było zgłaszać do urzędu ICO ani do rodziny. Zdarzenie musiało jednak zostać zapisane przez Hufcowego w wewnętrznym rejestrze naruszeń PSA UK Region, aby pomóc nam wyciągnąć wnioski na przyszłość.

Co Zrobić, Gdy Dojdzie Do Naruszenia Danych?

Według brytyjskiego prawa, jeśli dojdzie do poważnego wycieku danych, nasza organizacja ma bezwzględny czas **72 godzin** na zbadanie sprawy i zgłoszenie jej do urzędu ICO. Dlatego musisz działać **NATYCHMIAST**. Nie czekaj i nie oceniaj samemu czy sprawa jest „poważna”.

- **Krok 1:** Zauważasz wyciek lub utratę danych.
- **Krok 2:** Wypełniasz oficjalny formularz zgłoszeniowy online (link poniżej).
- **Krok 3: NATYCHMIAST ZAWIADAMIASZ** członka Zarządu PSA UK Region odpowiedzialnego za ochronę danych telefonicznie lub wiadomością SMS, a następnie wysyłasz e-mail do tego członka Zarządu (data.protection@zhpwb.org.uk) oraz do sekretariatu (admin@zhpwb.org.uk)

Kto i Jak Zgłasza Naruszenie?

- **Instruktorzy, Drużynowi i Wolontariusze (w każdym wieku):** NATYCHMIAST dzwonią lub wysyłają SMS do członka Zarządu PSA UK Region odpowiedzialnego za ochronę danych, wypełniają formularz online i wysyłają e-mail do Zarządu oraz sekretariatu.
- **Młodzież i Członkowie Poniżej 18 Lat:** Natychmiast zgłaszają sprawę rodzicom lub drużynowemu, aby ci mogli wypełnić formularz w ich imieniu.
- **Rodzice:** Jeśli zauważą naruszenie danych w naszych systemach, proszeni są o wypełnienie formularza online, co natychmiast zaalarmuje nasz sekretariat.

Oficjalny Link Do Zgłaszania Naruszeń

Aby zarejestrować naruszenie danych, wejdź na nasz bezpieczny formularz pod adresem:
<https://tinyurl.com/DPbreach>

Personal Data Breach Policy

Summary for Leaders/Instructors

This policy forms part of the governance framework of the Polish Scouting Association (UK Region) (known as PSA UK Region) to ensure full legal compliance with the UK General Data Protection Regulation 2018 (UK GDPR 2018) and the Data Protection Act 2018 (DPA 2018). As a registered UK charity and Data Controller, PSA UK Region is legally required to implement appropriate technical and organisational measures to protect personal data and uphold individual privacy rights. All leaders, instructors, and volunteers are required to understand and adhere to these statutory standards.

This document details exactly what constitutes a personal data breach and provides a step-by-step guide on how to report it if something goes wrong.

Because UK data law enforces strict reporting timelines, knowing how to spot and instantly escalate a data leak to PSA UK Region is critical for all leaders, instructors and volunteers.

What is a Personal Data Breach?

A data breach happens when personal information held by someone in PSA UK Region is accidentally or unlawfully lost, destroyed, altered, or accessed by the wrong person. This applies equally to paper records and digital files.

A data breach is not just about losing or leaking information. It also includes a security incident where personal data is made completely unavailable. For example, if a system failure, ransomware attack, or loss of access locks you out of your PSA UK Region Google Drive account so you cannot access emergency medical forms during a live event, this is legally classified as a data breach under UK law.

Two Scouting Case Studies: What to Learn

Case Study 1: Failing to hide a private address (High Risk)

What happened: A Troop Leader (Wodz Zuchow) sent a summer camp form to a cub's father to collect a missing signature. The leader forgot to block out the mother's new home address on the form. The mother had specifically requested that PSA UK Region keep her address private from her ex-partner for her own safety. The leader did not tell the mother about the mistake.

The outcome: Because the mother wasn't warned, she couldn't take safety precautions. The father turned up at her home, the police had to remove him, and the mother and child had to relocate.

The lesson: This was a severe breach that put someone in immediate danger. The leader should have informed the PSA UK Region Board and the mother immediately so she could protect herself. As the Data Controller, PSA UK Region was legally required to report this to the UK Information Commissioner's Office (ICO).

Case Study 2: Sending an email to the wrong leader (Low Risk)

What happened: A District Leader (Hufcowy) meant to email the BoyScouts Commissioner (Komendant Choragwi) about a family facing sudden financial and mental health difficulties, asking for a discount for an international jamboree. By mistake, the email was sent to the Girl Guides Commissioner (Komendantka Choragwi).

The outcome: The Girl Guides Commissioner immediately deleted the email and told the sender about the mistake. Because both leaders work within PSA UK Region, have data training, and handled it safely, there was no real risk of harm to the family.

The lesson: This did not need to be reported to the ICO or the family. However, the breach still had to be recorded internally, by the District Leader (Hufcowy) who had sent the email, on PSA UK Region's central breach log to help us improve our training.

What to Do If a Breach Happens

Under UK law, if a serious data leak occurs, our organisation has a **strict deadline of 72 hours** to investigate and report it to the ICO. Because of this, **you must act IMMEDIATELY**. Do not wait to see if it is "serious" before reporting it.

Step 1: You discover a data leak.

Step 2: Fill in the Official Online Reporting Form (Link provided below).

Step 3: ALERT the PSA UK Region board member responsible for Data Protection IMMEDIATELY via phone call or text message. And follow up with an email to the board member and administration

Who Reports the Breach?

- **Instructors and Volunteers (Any Age):** ALERT the PSA UK Region board member responsible for Data Protection IMMEDIATELY via phone call or text message. And follow up with an email to the board member and administration
- **Members under 18:** Tell your parent or your Unit Leader immediately so they can submit the form on your behalf.
- **Parents:** If you spot a data leak on our systems, please complete the online form below to alert our administration team.

Official Breach Submission Link

To record a data breach, access our secure form by copying and pasting this web address:

<https://tinyurl.com/DPbreach>

Agreed by Board of Trustees

Date: 9 September 2026

Review by date: 9 September 2027