JDP
Drapała &
Partners

GLOBAL COMPLIANCE, LOCAL RISKS

8 privacy hot spots to consider in Poland

Below we discuss Polish data protection regulations and common mistakes made by organisations with offices in Poland, where specific solutions are implemented by the headquarters in another country. In addition, we point out the potential consequences and how they can be prevented through the implementation of recommended solutions.

CONTENTS:

1. COOKIES AND OTHER TRACKING TECHNOLOGIES

POLISH SPECIFICITY

In Poland, the use of cookies and other tracking technologies is strictly regulated by the Electronic Communication Act (ECA) (Articles 399–400 ECA). Under these provisions, cookies may only be placed on the user's terminal equipment with the user's prior, active and express consent. Users must be able to have an option to consent to different categories of files (e.g. those necessary for the operation of the service, analytics, marketing) separately, and to easily withdraw their consent at any time.
The regulations require keeping a clear record of the consents given, including information on who, when and to what gave a consent, and specifying the maximum retention periods for each type of data. During an audit, the supervisory authority (Electronic Communication Office or Personal Data Protection Office) verifies, among other things, whether the consent banner allows all files to be rejected and whether the logs really archive the consent history in a way that guarantees full auditability.

COMMON MISTAKE

Global soft opt-in banner – one "Accept all" button, no option to opt-out or disable analytics cookies, consent recognised "by further use", no consent record or retention tables.

POTENTIAL CONSEQUENCES

- Penalty imposed by the Head of the Electronic Communication Office: up to 3% of revenue generated in Poland.
- Penalty imposed by the Personal Data Protection Office/under the GDPR: up to EUR 20 million or 4% of global turnover.
- Order to immediately disable scripts may result in a drop in conversions and loss of analytical data.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Cookie policy PL/EN + Consent banner PL/EN ("Accept / Reject / Settings")	Coherent, ready-to-use document; easy implementation by any web development team. Maintaining consistent UX across the group while fully complying with Polish requirements.
Quarterly compliance review checklists	Internal verification by the marketing team — reduces the need for further external audits and identifies non-compliance at an early stage.
Consent register + retention matrix	Ready-to-use proof of accountability to be presented to the Electronic Communication Office/Personal Data Protection Office; simplified internal reporting.
"Legal tags in 90 minutes" workshop for marketing and IT teams	Teams are able to internally maintain compliance in subsequent campaigns, which shortens "time to market" and reduces legal costs.

2. MARKETING COMMUNICATIONS (EMAIL, SMS, PUSH, INSTANT MESSAGING)

MARKETING COMMUNICATIONS (EMAIL, SMS, PUSH, INSTANT MESSAGING)

Any communication of a commercial nature – even if sent to a business address – requires the prior express consent of the recipient (Article 398 ECA).

The consent must be:

- separate from the acceptance of the terms and conditions or privacy policy,
- clearly documented (date, time, source),
- easy to withdraw, and the organisation is obliged to recognise the opt-out within 48 h,
- separate for each communication channel e.g. SMS, push, email, phone call).

COMMON MISTAKE

mass B2B cold mailing based on "legitimate interest" or a single combined checkbox for marketing consents. Lack of a central consent register and unsubscribe history.

POTENTIAL CONSEQUENCES

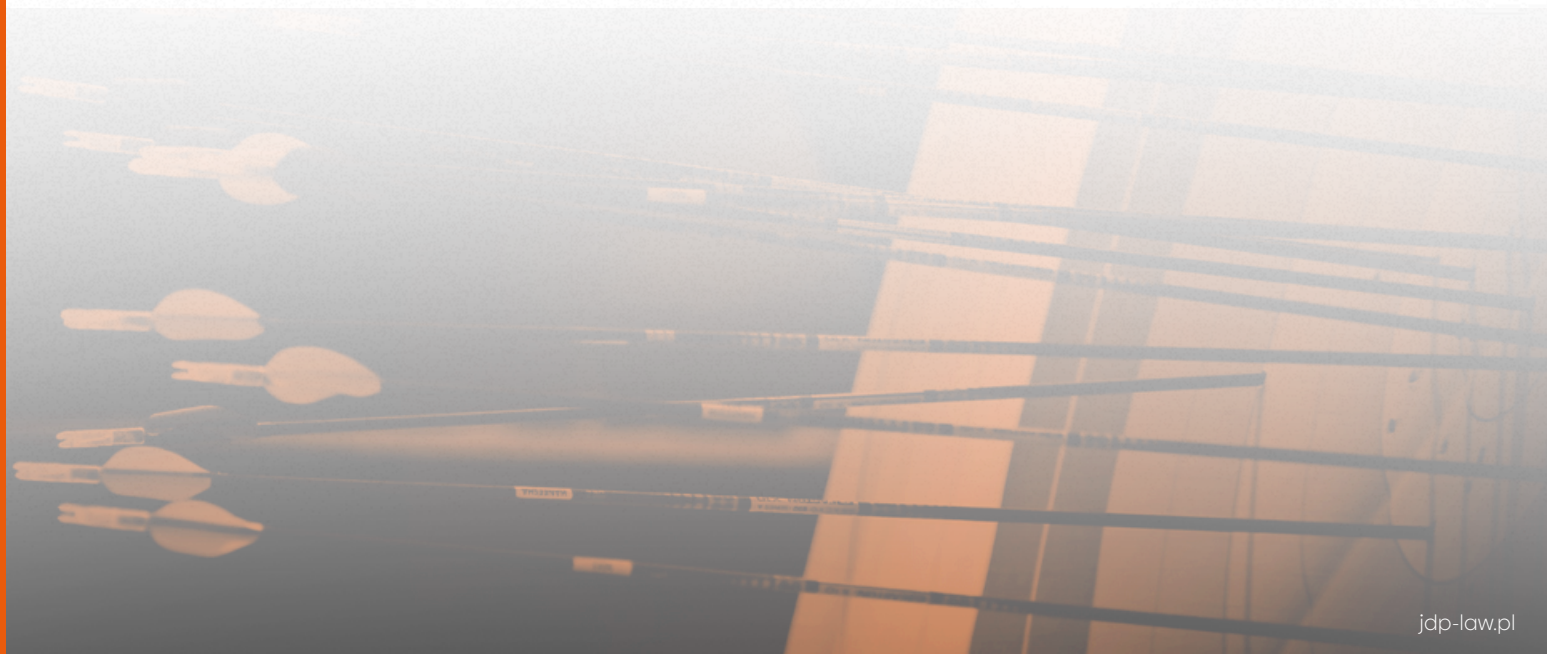
- Penalty imposed by the Head of the Electronic Communication Office: up to 3% of annual revenue generated in Poland.
- Penalty of up to PLN 2 million imposed by the Head of the Competition and Consumer Protection Office on a manager for deliberate action.

Market reference:

- Telecommunications operator – PLN 9.1 million fine for sending over 3.8 million marketing text messages without the required consents of the customers.
- PLN 80,000 fine for making over 30,000 marketing phone calls without the consent of the recipients.
- Telecommunications operator – PLN 2.85 million fine (2024) for making phone calls and sending marketing content via text messages and emails without the required consent.
- Telecommunications operator – PLN 5 million fine for direct marketing using automatic calling systems (advertising text messages) without the consent of the recipients, even when the activities were outsourced to an external entity.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Consent collection policy + "preference centre" mock-up (PL/EN, ready to use)	Standardised, legally compliant form with separate checkboxes; users see clear choices, which increases conversion rates and minimises the risk of violation of the Polish Electronic Communication Act.
Model consent register with instructions for integration with any CRM system	For each consent a date, source and scope are specified — in the event of an inspection by the Electronic Communication Office/Personal Data Protection Office, the legal team exports a report with a single click.
Opt-out procedure ("48-hour SLA opt-out") – instructions for marketing and IT teams + template email confirming opt-out	Quick removal of an address from the list reduces complaints, protects the domain's reputation and limits the risk of high administrative penalties.
One-page pre-campaign checklist (to be signed by the campaign owner)	Self-monitoring by the marketing team reduces the need for constant legal supervision and speeds up the launch of new mailings.
"Opt-in in 30 minutes" mini online training session (recording + PDF)	New employees quickly learn the rules, ensuring ongoing compliance without additional onboarding costs.



3. MONITORING OF EMPLOYEES AND VISITORS (CCTV AND EMAIL)

POLISH SPECIFICITY

Any form of workplace monitoring – including CCTV image recording, GPS location tracking and control of a business inbox – must be formally included in the work regulations in accordance with Article 22^2 of the Labour Code. The employer must inform employees of the planned implementation of the monitoring at least 14 days in advance and place appropriate signs in the areas covered by the monitoring. The purpose of the monitoring must be clearly defined (e.g. ensuring security, protecting property, maintaining the confidentiality of information) and any action must be proportionate to the intended purpose and in compliance with data protection regulations.

COMMON MISTAKE

Mail scanning tools used centrally in a corporate group, without considering the local legal environment for these technologies. Reading employees' emails without their consent through the IT team, without implementing monitoring.
A CCTV system without clear signage. GPS in cars without restriction of use. Monitoring of business phones without clear information.

POTENTIAL CONSEQUENCES

- Fine imposed by the Labour Inspectorate: up to PLN 50,000.
- Penalty imposed by the Personal Data Protection Office (e.g. EUR 160,000 for hidden surveillance of a medical facility).
- Claims for damages raised by employees for violation of personal rights or privacy.
- Necessity to consider the use of evidence obtained through illegal surveillance in a court dispute with an employee in terms of the consequences of such use.
- Criminal sanctions also possible: fines, restriction of liberty, even imprisonment for up to 2 years (Article 267 § 3 of the Criminal Code).

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
DPIA and update of Work Regulations (CCTV + email)	Monitoring is regulated in accordance with Polish law — evidence will be valid in the event of a dispute without the risk of recourse claims.
Proposal of signage, clauses and recording deletion schedule	Employees are properly informed, which reduces the risk of complaints to the Labour Inspectorate and the Personal Data Protection Office.
Protocol for accessing e-mail inboxes	HR and legal teams have a clear, approved procedure — allegations of "unauthorised surveillance" are avoided.

4. PRIVATE DEVICES AND COMMUNICATION TOOLS (BYOD)

POLISH SPECIFICITY

In the Polish legal environment, the employer may only authorise the processing of business data on employees' private devices after obtaining their written consent and conducting an appropriate risk assessment, considering the requirements of the GDPR and Article 22[1] of the Labour Code. It is also necessary to implement MDM (Mobile Device Management) solutions or other mechanisms to secure private devices, and the employment termination procedure must regulate the recovery or deletion of company data located on these devices.

COMMON MISTAKE

employees use private phones and computers for business purposes (BYOD), but the company has no established policy or written consent for this (no MDM). These devices are not adequately secured, and there is no procedure for recovering the company data stored on them if an employee leaves.

POTENTIAL CONSEQUENCES

- Penalty imposed under the GDPR: 4% of global turnover.
- Potential criminal liability on the part of executives (Article 107 of the Personal Data Protection Act) for disclosing
- Loss of control over trade secrets (e.g. customer database on a private drive).

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
BYOD and messengers policy + consent templates	Employees and managers have clear rules, which minimises the risk of data leakages.
MDM/encryption requirements list + "lost phone" playbook	Mobile incidents are quickly dealt with, which can prevent a report to the Personal Data Protection Office and a penalty.
"Secure Messaging" workshop	Sales and customer service teams use messengers in line with the law and industry requirements.

5. WHISTLEBLOWERS

POLISH SPECIFICITY

The Polish Whistleblowing Act from 2024 requires that all whistleblowing reports are received and handled by a dedicated unit operating in Poland. The organisation must provide appropriate organisational and technical safeguards, and in the case of using an external SaaS platform, should enter into additional agreements to ensure that reports are handled in line with Polish regulations and that timely feedback is provided to the whistleblowers.

COMMON MISTAKE

A whistleblower channel operated only in the headquarter (e.g. Germany), with no local procedure, no Polish decision-making team and no timely feedback.

POTENTIAL CONSEQUENCES

- Administrative fine: up to PLN 50,000 for failure to put in place the procedure or its incorrect implementation.
- Criminal liability (fine, restriction of liberty, imprisonment of up to 3 years) for retaliatory actions.
- Reputational damage after disclosure to the media or external authorities.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Global channel localisation (DPIA, PL procedure, report register)	The company complies with the statutory requirements without having to replace its entire IT platform.
Training for the report committee	Decisions are made quickly and in accordance with the law, which minimises criminal and reputational risks.
“Dry-run” – incident test	Team knows the procedure in practice and any gaps are fixed before they are reported.

6. DATA PROTECTION POLICIES AND INDIVIDUAL AUTHORISATIONS

POLISH SPECIFICITY

The supervisory authority (Personal Data Protection Office) in its decisions repeatedly emphasises that each employee must have an individual authorisation to process personal data, specifying the scope of activities and the systems they are authorised to process. The data protection policy should reflect the organisational structure of the company, define the persons responsible for handling requests from data subjects (response time – 30 days), the incident management procedure (response within up to 72 hours) and be implemented separately in each company. This documentation is key evidence of accountability in the event of an audit.

COMMON MISTAKE

A global policy implemented "by email", without a resolution of the management board of a Polish company and without individual authorisations; no incident register.

POTENTIAL CONSEQUENCES

- Decision of the Personal Data Protection Office: PLN 40,000 for lack of documentation and order to stop processing until the documentation is completed.
- Operational chaos during an incident – unclear roles slow down response, increasing the risk of financial penalties.
- Most penalties imposed by the Personal Data Protection Office concern the failure to document violations and notify data subjects, e.g. a bank was fined over PLN 363,000 for failing to notify customers about a personal data leakage.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Editable, scalable authorisation form (Word/Excel)	Quick generation of a set of personal authorisations – a requirement specified in the Personal Data Protection Office's decisions, without the HR team having to prepare the documents manually.
Management board's resolution + updated data protection policy	Documentation duly adopted by the Polish entity; positively assessed by supervisory authorities during compliance checks.
Review of group procedures and "local supplement" – summary of discrepancies PL vs global standard	Corporate processes are maintained, while requirements specific to Polish law are clarified and supplemented; this minimises the risk of jurisdictional conflicts and facilitates internal audits.
Procedure for exercising data subjects' rights and incident register (workflow + register sheet)	Clear, approved workflow for requests and events reduces response times, lowers the risk of penalties for delays, and enables reporting to the management board in a transparent format.

7. DATA PROTECTION OFFICER (DPO)

POLISH SPECIFICITY

In Poland, a DPO must be a designated natural person reported to the Personal Data Protection Office by a Polish company. If this role is entrusted to an external organisation, it is necessary to designate a specific employee of this organisation as the responsible DPO. His or her contact details – including forename and surname – must be provided in Polish on the website and in privacy notices. The DPO should report directly to the management board and have the resources necessary to fulfil his or her duties, and should speak Polish or have the support of a Polish-speaking team.

COMMON MISTAKE

One person acting as a global DPO is not formally reported in Poland; no contact details in Polish on the website; DPOs also performing other roles – conflict of interest.

POTENTIAL CONSEQUENCES

- Penalty imposed by the Personal Data Protection Office: PLN 25,000 (example for 2024) for failure to report a DPO.
- Possible penalties of up to 2% of global turnover (GDPR) for more serious violations.
- Order to appoint a new DPO and again inform all data subjects.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Online DPO report within 24 hours	Risk of a penalty for failure to report is eliminated immediately.
Outsourcing agreement or "shadow DPO support"	Global DPO benefits from local language support and operational assistance from the law firm, without having to hire new staff.
Annual work plan for DPO + KPI dashboard	The management board receives measurable compliance reports, which facilitates supervision and budgetary decisions.

8. ANNUAL REVIEW OF THE DATA PROTECTION SYSTEM

POLISH SPECIFICITY

Pursuant to the accountability principle under Article 24 GDPR, each organisation is required to conduct a documented review of the effectiveness of the implemented data protection measures annually or after any significant change in the IT environment (e.g. new system, company acquisition). According to the Personal Data Protection Office's decisions, it is required to have an audit report with recommendations for corrective measures approved by the management board, to demonstrate full compliance during a possible inspection.

COMMON MISTAKE

Policies implemented in 2023 have not been updated and new applications and providers have not been assessed at all; internal audit is limited to a "copy-paste" checklist.

POTENTIAL CONSEQUENCES

- Outdated procedures result in incidents not being detected or reported late.
- Maximum penalty under the GDPR, depending on the violation: 2% or 4% of global turnover.

OUR SOLUTIONS – VALUE FOR THE CLIENT

What we do	Tangible benefits
Risk-based audit methodology and 12-month schedule	Review tailored to real business risks, not a "paper formality".
"Audit in 60 minutes" sheet – department self-assessment	Heads of individual divisions can quickly assess compliance internally; a central data team receives standardised results without the need for lengthy meetings.
"Table-top" workshop for the management board	Management will drill control or incident scenarios, which will reduce response times in critical situations.

CONTACT

Anna Matusiak-Wekiera

Attorney-at-law | Counsel, Head of Data Protection & Compliance

E: anna.matusiak-wekiera@jdp-law.pl

Krzysztof Brant

Attorney-at-law | Senior Associate, Data Protection & Compliance

E: krzysztof.brant@jdp-law.pl

JDP Drapała & Partners

JDP DRAPAŁA & PARTNERS Sp. k. / KRS: 0001145849 / Registry Court: District Court for the Capital City of Warsaw in Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753