

Guides — infrastructure planning and maintenance

Practical DATPOL checklists: property services, SOMAG, agriculture, audits, LCPD and SOC.

- [How to hand over property services to DATPOL One](#)
- [How to report a fault so engineers can respond effectively](#)
- [How to build a property maintenance plan](#)
- [How to prepare a sports lighting enquiry](#)
- [What to check before deploying LoRaWAN lighting control](#)
- [How to prepare a farm for a standby power assessment](#)
- [How to prepare a business for an audit without disrupting operations](#)
- [How to compare an indoor server room with a container solution](#)
- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)
- [Information Security Management System \(ISMS\) — a practical implementation guide](#)
- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)
- [EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation](#)
- [Opomiarowani — sensors, alerts and measurement history explained](#)
- [EMS for local authorities — energy across schools, offices and municipal sites](#)
- [EMS for businesses — from consumption profiles to an improvement plan](#)

How to hand over property services to DATPOL One

[Czytaj po polsku](#)

A practical handover plan covering scope, records, responsibilities and initial priorities.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Define the service boundary

List the buildings, grounds and systems to be covered. Separate routine work from upgrades and purchases. Identify warranties and manufacturer service agreements. A single contract does not automatically mean unlimited work or a round-the-clock duty service.

Prepare the handover

Gather asset records, inspection reports, manuals, schedules and outstanding faults. Identify spending approvers and site access procedures. Transfer credentials through an agreed secure channel, never in an ordinary support ticket.

Agree the first work plan

Agree urgent defects, the maintenance schedule and reporting arrangements. Record who receives requests, assigns priority and approves extra work. DATPOL One combines technical services and maintenance coordination within the scope agreed for each property.

Practical checklist

- Properties and systems.
- Records, warranties and outstanding faults.
- Service hours, escalation and spending limits.
- Report format and named approver.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to report a fault so engineers can respond effectively](#)
- [How to build a property maintenance plan](#)
- [How to prepare a business for an audit without disrupting operations](#)

How to report a fault so engineers can respond effectively

[Czytaj po polsku](#)

A useful request records symptoms and business impact without guessing the cause.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Record facts

Give the location, equipment name, first occurrence and last known working time. Copy the exact error message. Explain whether one person, one room or the whole property is affected. Mention recent work or power interruptions.

Explain the impact

Describe the activity that has stopped and any safe workaround. Priority depends on the effect on people and operations, rather than simply labelling a request urgent. For immediate danger, follow site emergency procedures and contact the appropriate emergency services.

Attach evidence and a contact

Include a photograph of the equipment label and error if safe to obtain. Remove credentials and unnecessary personal information. Name an on-site contact and access hours. Avoid repeatedly resetting equipment and

losing fault evidence.

Practical checklist

- Site, equipment, time and symptoms.
- Scope and operational impact.
- A photo or error message without confidential data.
- Contact and access arrangements.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to hand over property services to DATPOL One](#)
- [How to build a property maintenance plan](#)
- [How to prepare a business for an audit without disrupting operations](#)

How to build a property maintenance plan

[Czytaj po polsku](#)

From an asset register to a schedule, completion evidence and overdue work tracking.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Start with an asset register

Give each item an identifier, location, model and responsible person. Add its records, warranty and service provider. Do not assign the same inspection interval to every system: intervals depend on equipment, instructions, operating conditions and applicable requirements.

Define the task and evidence

Record the activity, competent person, due date and evidence required, such as a report or measurement. Distinguish user checks from inspections requiring qualifications. Allow for isolation, access and return to service.

Track findings to closure

Completing an inspection does not automatically resolve its findings. Give each corrective action an owner, deadline and verification method. A monthly report should cover completed tasks, overdue work, recurring faults and budget decisions.

Practical checklist

- Asset register and records.
- Basis and due date for each task.
- Assigned provider and report.
- Corrective actions with deadlines.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to hand over property services to DATPOL One](#)
- [How to report a fault so engineers can respond effectively](#)
- [How to prepare a business for an audit without disrupting operations](#)

How to prepare a sports lighting enquiry

[Czytaj po polsku](#)

Information needed for a lighting concept and a meaningful comparison of quotations.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Describe how the pitch is used

Specify the sport, dimensions, operating hours, competition level and any broadcast requirements. Recreation and competition can require different designs. Compare more than lamp count, wattage or unit price.

Show the site constraints

Provide a plan, photographs and details of existing columns and power supplies. Identify nearby buildings and areas sensitive to spill light. Reusing structures requires assessment; replacing luminaires does not confirm that columns or foundations are sound.

Agree acceptance criteria

The quotation should state calculation assumptions, work scope, control scenarios and documentation. Agree acceptance measurements and functional checks. Energy-saving claims need a stated comparison with the existing installation and operating hours.

Practical checklist

- Plan and intended use.
- Column photographs and available installation records.
- Surroundings and work constraints.
- Calculations, measurements and documentation in the quotation.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [What to check before deploying LoRaWAN lighting control](#)
- [How to build a property maintenance plan](#)

What to check before deploying LoRaWAN lighting control

[Czytaj po polsku](#)

A pilot checklist covering luminaires, connectivity, failure behaviour and maintenance responsibilities.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Check the complete communication path

The luminaire controller, gateway and network server are separate parts of the solution. Verify radio coverage on site. Seeing a device in an application does not itself prove that a command changed the light output. Identify the acknowledgements and measurements the hardware actually provides.

Specify failure behaviour

Describe operation after loss of connectivity, power failure and restart. Require a description of any local schedule and manual operation. Do not assume all controllers provide the same functions.

Accept the pilot before expansion

Test representative locations and scenarios. Agree updates, account ownership, data export and ongoing costs. Describe lighting and any camera power supply separately so switching a lighting circuit cannot unintentionally stop equipment that needs continuous power.

Practical checklist

- Luminaire and controller compatibility.
- Coverage test results.
- Local and manual operation.
- Acceptance tests and ongoing costs.

Next steps and references

[DATPOL service scope and supporting material](#)

[LoRa Alliance — back-end interfaces](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to prepare a sports lighting enquiry](#)
- [How to build a property maintenance plan](#)

How to prepare a farm for a standby power assessment

[Czytaj po polsku](#)

An equipment and priority list supports a realistic assessment of standby power needs.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Identify critical processes

List equipment whose loss has the greatest impact, such as cooling, ventilation, water systems or controls. Provide nameplate details and tolerable interruption time. Adding rated power alone does not capture every starting condition.

Separate uninterrupted operation from long runtime

Some loads need continuity through short interruptions; others need hours of operation. Selecting a UPS, generator and transfer arrangement requires assessment of the installation and its operation. Never feed a building through a socket or use a generator without a properly designed supply transfer arrangement.

Plan operation and tests

Agree equipment location, service access, fuel, ventilation and operation in accordance with documentation. Arrange load tests with specialists and the people responsible for affected processes. Acceptance should cover restoration of normal service as well as starting the backup source.

Practical checklist

- Loads, ratings and priorities.
- Tolerable interruption and required runtime.
- Available electrical documentation.
- Location and operating arrangements.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to build a property maintenance plan](#)
- [How to prepare a business for an audit without disrupting operations](#)

How to prepare a business for an audit without disrupting operations

[Czytaj po polsku](#)

Agree scope, authorisation, records and report acceptance before work begins.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Define the question the audit must answer

Is the focus installation reliability, IT security, physical protection or an upgrade? Identify sites and processes. Put any specific compliance criteria in scope: a general review does not automatically establish compliance.

Separate inspection from active testing

Agree document access, interviews and visual inspections. Scanning, penetration testing, isolation and failure simulations require defined authorisation, a work window and stop conditions. Permission for an audit is not permission for every intervention.

Accept an action plan

The report should connect each observation with evidence, impact and a recommendation. Ask for priorities, action owners and a distinction between urgent repairs and capital work. Ensure assessment limitations are recorded.

Practical checklist

- Objective, sites and scope.
- Records and interview contacts.
- Authorisation and testing limits.
- Report format and follow-up verification.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to compare an indoor server room with a container solution](#)
- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)

How to compare an indoor server room with a container solution

[Czytaj po polsku](#)

Compare the complete project and operation, not just the room or container price.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Record common assumptions

Use the same IT load, expansion allowance, availability target, power and cooling requirements for both options. Without a common baseline, similarly named quotations may cover very different work.

Check location and dependencies

For a room, assess space, installation routes and work access. For a container, include land, delivery access, foundations, connections and approvals. A separate structure does not automatically remove a shared power dependency or single network connection. Determine formal requirements for the actual site and intended use.

Compare lifecycle costs

Include design, construction, connections, equipment, acceptance, energy and maintenance. Specify system migration, documentation and recovery tests. The programme must include dependencies and connection availability; delivery of a container does not mean services are operational.

Practical checklist

- Common assumptions for both options.
- Location, connections and dependencies.
- Capital and operating costs.
- Migration, acceptance and commissioning plan.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to prepare a business for an audit without disrupting operations](#)
- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)

What to prepare before connecting a public authority to a SOC

[Czytaj po polsku](#)

Inventory, log sources, authorisation and response testing before service acceptance.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Describe the environment and owners

List sites, systems, servers, endpoints, network devices and suppliers. Identify owners and critical services.

Agree log sources, time synchronisation and secure transfer. No events may indicate a missing integration rather than absence of threats.

Agree response authority

Record contact channels, service hours, priorities and actions needing approval. Automated blocking can interrupt work, so it needs an approved rule, exceptions, an audit trail and an unblock procedure. An alert is not the same as a confirmed intrusion.

Test the whole event workflow

Using an agreed scenario, test event delivery, detection, notification and documented response. Accept a list of active integrations and gaps. A SOC supports detection and response; it does not replace risk management, backups or all of an organisation's obligations.

Practical checklist

- Inventory and critical services.
- Log sources and delivery tests.
- Contacts, escalation and approved actions.
- Acceptance record and outstanding gaps.

Next steps and references

[DATPOL service scope and supporting material](#)

[CISA — Use Logging on Business Systems](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to prepare a business for an audit without disrupting operations](#)
- [How to compare an indoor server room with a container solution](#)
- [How to document a backup recovery test](#)

How to document a backup recovery test

[Czytaj po polsku](#)

A readable backup file is only the start: verify restoration of a usable service.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Define the scenario and acceptance criteria

Choose a specific service and recovery point. Agree tolerable data loss and restoration time: RPO and RTO. Test in an isolated environment or approved work window without risking production data.

Restore dependencies

Recovery may require configurations, keys, accounts, DNS and dependent applications as well as data. Keep secrets out of public test records. Check service startup and an agreed business operation; a matching archive checksum does not prove the application works.

Record results and corrective action

Record the backup, dates, timings, scope, operator, test outcomes and limitations. Do not describe a partial exercise as a test of every system. Assign fixes and retests for failures. Protect backups from incidents affecting the production environment.

Practical checklist

- Scenario, RPO and RTO.
- Safe test environment.
- Functional check by the service owner.
- Record, limitations and corrective actions.

Next steps and references

[DATPOL service scope and supporting material](#)

[CISA — StopRansomware Guide](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to prepare a business for an audit without disrupting operations](#)
- [How to compare an indoor server room with a container solution](#)
- [What to prepare before connecting a public authority to a SOC](#)

Information Security Management System (ISMS) — a practical implementation guide

[Czytaj po polsku](#)

An Information Security Management System (ISMS, known in Polish as SZBI) brings together leadership, people, procedures and technology to protect information across an organisation. This guide explains how to turn written commitments into working controls and evidence.

Prepared by DATPOL · updated 5 October 2026. For public authorities, their associated organisations and businesses. This British English edition concerns organisations operating in Poland; it does not claim compliance with UK legislation. Suggested schedules, risk scales and review intervals are organisational examples unless a specific legal requirement is identified. This is not an individual compliance assessment.

1. What is an ISMS?

An ISMS is an agreed, documented and continually improved approach to information security. It covers electronic records, paper documents, conversations, staff knowledge and information handled by partners. It combines responsibilities, processes and technical measures.

Its central objectives are **confidentiality** — access by authorised parties; **integrity** — protection against unauthorised alteration; and **availability** — information and services being usable when required. Accountability and trustworthy sources also matter.

For example, a member of staff must access the correct case file, an invoice payment account must not be altered fraudulently, and a council must continue serving residents after a server failure. Each objective requires different controls.

2. ISMS, ISO 27001, KRI, KSC, NIS2 and GDPR

- **ISO/IEC 27001:2022** specifies requirements for a risk-based ISMS. Certification is a separate process: an organisation can implement an ISMS without a certificate. Certification has a defined scope and does not guarantee that incidents will never occur. [ISO source](#).
- **Polish KRI:** section 19 of the regulation of 21 May 2024 provides for an ISMS in bodies performing public tasks. Section 19(2)(14) requires an internal information security audit at least annually. Its reference to an ISMS based on PN-ISO/IEC 27001 and related standards should not be confused with a blanket requirement to buy certification. [KRI source](#).
- **KSC and NIS2:** Poland's KSC amendment implementing NIS2 entered into force on 3 April 2026. Determine obligations for the specific legal entity, activities and statutory classification. Do not assume every school, municipal company or associated body has the same status. [Ministry source](#).
- **GDPR** addresses personal data; an ISMS also protects other information. Coordinate controls and evidence, but do not treat one programme as automatic compliance with the other. [GDPR, particularly Articles 32–34](#).

At the review date: official guidance identifies 3 October 2026 for registration of the relevant group and 3 April 2027 for implementing new duties for entities meeting the criteria when the amendment entered into force. The first date has already passed. Check whether entry is automatic or application-based and verify your own status. Transitional arrangements do not remove earlier KRI or data-protection obligations. [Official timetable](#); [KSC duties and criteria](#).

3. Define scope, services and accountability

Identify organisational units, sites, staff, remote working, applications, suppliers and business processes. Explain exclusions. A scope described simply as “all IT” can overlook paper archives, contractors and hosted services.

For a municipality with 25 office staff, assess the council office, school, nursery, childcare centre, cultural centre, cemetery and community premises separately. Shared IT support does not automatically create a single data controller or transfer directors' responsibilities. Common standards can help, provided ownership remains explicit.

- **Leadership:** approves scope, resources, priorities and risk acceptance.

- **ISMS coordinator:** maintains the programme, records and reviews.
- **Process owners:** define information needs and the consequences of disruption.
- **IT and suppliers:** implement agreed controls and provide operational evidence.
- **Data protection officer:** retains their independent data-protection role; they do not automatically become the IT administrator or owner of the whole ISMS.
- **Staff:** follow practical rules and report concerns through a familiar channel.

4. Inventory: what are you protecting?

Cover endpoints, servers, phones, networks, applications, licences, accounts, certificates, domains, backups, archives and external services. Record ownership, location, purpose, information category, dependencies, support expiry and maintenance responsibility. Include CCTV, access control and building automation.

An inventory agent can discover equipment and installed software. It cannot independently establish business criticality, lawful processing grounds or licence entitlement. Compare installations with contracts and purchasing evidence. Assign a register owner and update records when assets are acquired, changed or retired.

5. Information classification and everyday work

Use understandable categories such as public, internal and confidential. Define permitted storage, sharing, encryption and disposal for each. This internal scheme does not replace statutory classified-information categories.

Staff should know whether they may send a document through a personal messenger, use a private USB drive or enter case information into a public AI service. Identify approved tools and an exception process. If a rule cannot realistically be followed, improve the workflow rather than merely requesting another signature.

6. Assess risk step by step

1. Select a service or asset and identify its owner.

- 2. Describe a scenario: threat, weakness and organisational consequence.
- 3. Account for controls that actually operate.
- 4. Assess likelihood and impact using a documented method.
- 5. Choose treatment: reduce, avoid, share or knowingly accept the risk.
- 6. Assign delivery ownership, resources, deadline and completion evidence.
- 7. Reassess residual risk and obtain an authorised decision.

A 1–5 scale and multiplied score can assist prioritisation, but the number cannot replace reasoning. Consider residents, personal safety, service continuity, confidentiality, finances and obligations. Review risk after significant changes and incidents as well as on a planned cycle.

Illustrative risk-register entry

Field	Example
Process and owner	Payroll; payroll manager
Scenario	A compromised administrator account permits encryption of the server and connected backups
Impact	Delayed salary processing and possible disclosure of staff information
Treatment	MFA, separate administrator accounts, isolated backup and recovery exercise
Evidence and decision	Configuration checks, successful application test and documented residual-risk acceptance with review date

7. Documentation that supports action

A practical set includes the policy, scope, responsibilities, asset register, risk method and register, treatment plan, access rules, backup procedures, change and patch processes, incident management, continuity, supplier requirements and user guidance. Include a register of legal and contractual obligations and an audit and training plan.

Give documents an owner, version, approval, review date and intended audience. A completed leaver-access checklist provides stronger operational evidence than a general statement that accounts are protected. For an ISO 27001 implementation, prepare a Statement of Applicability with justified control decisions; check full requirements against a current, lawfully obtained copy of the standard.

8. Access, MFA and remote administration

Use individual accounts and task-appropriate privileges. Separate administration from everyday work. Prioritise MFA for email, remote access, administration and backup systems, and test recovery and emergency-access arrangements.

Process owners authorise access. Staff departure or role change triggers removal or adjustment. Reviews must include suppliers, service accounts, API keys and obsolete integrations. Supplier access needs a defined scope, expiry and activity record. Store credentials in an appropriate secrets system, never in a public knowledge base or an ordinary support ticket.

9. Patching, segmentation and physical security

Prioritise fixes according to exposure and potential impact. Changes need ownership, verification and a rollback plan. Unsupported systems require replacement decisions or documented compensating controls with review dates.

Separate administrative systems from guest Wi-Fi, cameras and technical devices. Permit communication according to service needs. Assess server-room access, power, temperature, water ingress and appropriate fire protection. Select measures through risk assessment and design: buying a camera or door lock does not establish compliance with all KSC duties.

10. Backups and continuity

The service owner defines RPO, the tolerable period of lost data, and RTO, the target recovery time. Protect backups against failure or compromise of production. The 3-2-1 approach is useful guidance, not a universal statutory prescription or proof that a backup design works.

Recovery testing should restore data, configuration and dependencies, start the application and complete an agreed business task. A matching archive checksum verifies file integrity, not service usability. Record achieved

recovery objectives, limitations and corrective action. Plan degraded operations too: communication with residents, manual intake and later reconciliation.

11. Logs, SOC and automation

A SOC supports event monitoring, alert analysis, escalation and agreed response. Define its visibility, operating hours, escalation recipients and authority. A continuously running platform is different from a staffed 24/7 analyst service.

Check log-source coverage, time synchronisation, access and justified retention. No alerts can mean missing data. Automated blocking needs approved rules, exceptions, an audit trail and an unblock procedure. AI output supports investigation; it is not independent proof of an incident or a compliance decision. Keep organisational data within the agreed environment and processing scope.

12. Incident management

Provide one simple reporting channel. The responder records timing, symptoms, affected services and actions, then escalates appropriately. Authorised personnel contain the incident and preserve evidence. Do not direct ordinary users to delete files, reinstall systems or send confidential information to private addresses.

Combine technical classification with assessment of KSC, personal-data and contractual reporting duties. Do not apply one deadline to every notification. Identify recipients, the event that starts the relevant clock, deputies and approval responsibilities. Closure includes confirmed recovery, cause analysis and completed corrective actions.

13. Suppliers, cloud and external processing

Assess supplier access, processing locations, subcontractors, support, response times, backup responsibilities and data export at contract end. Agree incident notification and evidence of service delivery. "Secure cloud" does not identify who restores an accidentally deleted register.

Before adopting remote management or an AI model, establish what information it receives, the processing basis and safeguards. Do not combine independent customers' information in a shared account without an agreed separation and access model.

14. People and training

Induction should cover authentication, email, reporting concerns, documents and devices. Managers also need decision exercises: who authorises taking a system offline, communicates with residents and approves degraded operations?

Short refreshers and scenario exercises reveal behaviour better than attendance records alone. Teach staff to verify changes to bank details through a known independent channel. Encourage prompt, honest reporting of mistakes.

15. An illustrative first 90 days

A starting plan, not a guaranteed delivery time

Period	Work	Output
Days 1–15	Scope, ownership, units, urgent gaps and requirements	Approved programme and service owners
Days 16–30	Inventory, risks, accounts, backups and suppliers	Registers and prioritised actions
Days 31–60	Procedures, controls, monitoring and training	Implementation evidence and outstanding gaps
Days 61–90	Recovery exercise, incident exercise, audit and management review	Test results, decisions and corrective plan

Complex estates, public procurement and missing records may extend implementation. Address the most serious risks and maintain an honest gap list. Do not declare completion while basic tests or accountable owners are missing.

16. Effectiveness and audit readiness

Define measures with clear denominators: critical services supplying logs, privileged accounts protected by MFA, recoveries checked at application level and overdue risk actions. “All agents online” ignores equipment that was never inventoried.

Audits need criteria, scope, competence and impartiality. Vulnerability scans and penetration tests support technical assurance but do not replace an ISMS audit. Leadership reviews results, incidents, risks and resources, assigns actions and checks completion. Monthly operational and quarterly risk reviews are possible starting points; determine actual frequency from needs and applicable obligations.

17. Acceptance checklist

- Approved scope, responsibilities and deputies.
- Current asset, service, owner and supplier registers.
- Documented legal applicability and obligations.
- Risk register and agreed treatment plan.
- Tested access provisioning and removal.
- Recovery reports for selected services, including limitations.
- Tested escalation and out-of-hours contact where required.
- Log-source coverage and SOC response authority.
- Staff understanding and exercise evidence.
- Audit results, management decisions and dated corrective actions.

18. Common questions

Can we simply buy policies? Policies need to reflect the real environment, have owners and be used in practice.

Does buying a SOC deliver an ISMS? It covers part of the technical and operational work, not the organisation's entire governance.

Does certification prove compliance with every law? No. Scope, criteria and validity matter; legal duties require separate assessment.

Does a small body need a large team? Resources should match risk. Shared or external support is possible, but accountability and availability must be explicit.

What does implementation cost? It depends on units, services, infrastructure condition and gaps. Separate assessment and documentation from licences, replacements, monitoring, tests, training and ongoing maintenance. A cheap document pack does not describe the cost of operational readiness.

19. Preparing a discussion with DATPOL

Bring site and user numbers, critical services, IT-support arrangements, backup information and known issues. These support agreement on assessment, priorities and technical work covering networks, server rooms, physical protection, recovery and monitoring integrations. Tasks, service hours and responsibilities must be agreed contractually.

[SOC monitoring and response](#) · [LCPD server-room construction and modernisation](#) · [DATPOL24 contact and service requests](#). Do not submit passwords, full configurations or residents' information through a public form.

Related guides

- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)
- [How to compare an indoor server room with a container solution](#)
- [How to prepare a business for an audit without disrupting operations](#)

Podlicznik — meter readings, tenant charges and reports: a property manager's guide

[Czytaj po polsku](#)

Podlicznik by DATPOL helps property managers organise electricity readings and prepare tenant charge statements for commercial premises, hotels and apartments. This guide covers the current portal, not an assumption that remote meters are already connected.

[Product website \(Polish\)](#) · [Client portal](#) · podlicznik@datpol.com

1. Current scope

The portal supports premises, meters and tenants, manual readings, net rates, charge statements, CSV export, browser printing to PDF, activity history and scheduled email reports. Remote meter/gateway integration requires commissioning for each property. Adding a serial number does not establish a connection. An AI forecasting model is not yet connected; forecasts must never replace actual readings for billing. The public demo uses fictional data and sends no emails.

2. Prepare for commissioning

Prepare a list of properties and units, meter models and serial numbers, tenant assignments, verified cumulative readings and dates, agreed net rates, billing periods, recipient addresses and authorised managers. Confirm any measurement multiplier with DATPOL: the current form expects the correct cumulative kWh value and has no separate transformer-ratio field. Agree additional charges, accounting integration, retention, backups and maintenance separately.

3. Sign in

Use an authorised email address through Cloudflare Access. The account must also be assigned to an organisation inside the application. Receiving a sign-in code does not grant access to every organisation. If your account has no organisation, contact DATPOL with your email and organisation name, never a password or login code. The portal supports separate organisations and two roles. Managers can manage only their own organisation's meters. Tenants have read-only access to explicitly assigned meters, readings within their tenancy dates and their own statements. They cannot see other units, organisation settings, manager activity or whole-supply reconciliation. DATPOL provisions the account and its dated meter assignments; an email recipient address alone never grants portal access.

4. Add premises and meters

In the Polish interface, select **Lokale i liczniki ? Dodaj licznik**. Enter the property, unit, serial number, tenant, optional tenant email and net rate in PLN/kWh. Use unambiguous unit names. The current interface does not provide self-service changes of tenant, meter replacement or edits to saved register entries. Ask DATPOL to make these changes while preserving history; do not create a second entry to hide a mistake.

5. Add actual readings

Select **Odczyty ? Dodaj odczyt**. Enter the cumulative meter register in kWh, not consumption for the month. For example, an opening reading of 1000 kWh and closing reading of 1426 kWh represent 426 kWh consumed. Future dates, duplicate readings for the same meter and date, and values inconsistent with earlier or later readings are rejected. Meter replacement or rollover requires separate verification; do not invent an acceptable value.

6. Create a charge statement

Select **Rozliczenia ? Utwórz zestawienie**, choose the meter and period boundaries, check the net rate and save. Actual readings must exist for both exact boundary dates. At 1.10 PLN/kWh, 426 kWh gives **468.60 PLN net**. Saved statements retain the readings, rate and tenant details used at creation. Overlapping periods are blocked; an incorrect existing statement needs a correction arranged with DATPOL, not a second overlapping charge.

A statement is **not a VAT invoice**. Current calculations exclude tax and additional fixed or distribution charges. Accounting integration and more complex tariffs are separate implementation requirements. This English version describes a deployment in Poland and does not imply compliance with UK billing rules.

7. Export CSV or PDF

Use CSV beside a saved statement to download its data. PDF opens a printable view; choose “Save as PDF” in the browser print dialog. If necessary, allow pop-ups only for the portal. Exports contain tenant information and should only be shared with the appropriate recipient.

8. Enable monthly emails

Open **Raporty e-mail**, enter the manager's email, check tenant addresses and meter rates, then enable and save the schedule. It is disabled by default. The job runs daily at 08:15 Polish local time and checks the previous calendar month. September requires readings dated 1 September and 1 October. Missing readings or an overlapping custom-period statement prevent automatic processing for that meter.

The schedule uses the meter's saved rate; an existing report keeps its own rate. Messages include a statement and CSV attachment. The manager and relevant tenant receive separate messages. A tenant without an email address receives no copy. Sender and reply address: **podlicznik@datpol.com**.

“Przyj?te przez SMTP” means accepted by the mail server, not read by the recipient. “Do sprawdzenia” requires investigation; uncertain sends are not retried automatically to avoid duplicates. Disabling the schedule does not recall messages already sent.

9. Analysis and troubleshooting

The analysis view totals saved statements by the month in which each period starts; it is not yet a continuous telemetry chart. Compare equivalent periods and consider occupancy, tenant changes and equipment.

- **No readings:** check the meter assignment and whether remote integration has actually been commissioned.
- **Cannot create a statement:** check exact boundary readings and existing reports.
- **Unexpected charge:** review opening and closing values, units and rate. Do not compare a net statement directly with a gross invoice containing other charges.

- **No email:** check schedule settings, recipient address, queue status and spam folder. Avoid repeated manual sends.
- **Sudden increase:** verify the period and source readings; a rise alone does not establish a fault or misuse.

10. Security and support

Cloudflare Access, HTTPS, server-side token checks, organisation assignments and an activity history protect the portal. These are controls, not an absolute security guarantee. Permissions, updates, retention and backups require agreed operational arrangements.

Contact [DATPOL24](#), podlicznik@datpol.com or [+48 55 621 29 29](tel:+48556212929). Include the property, unit, meter serial, period, error text and report number where available. Never send passwords or sign-in codes. Do not open electrical cabinets or interfere with wiring to obtain a reading; use appropriately qualified personnel.

Feature status checked against the deployment on 6 October 2026. The service scope is agreed for each property.

Related guides

- [How to hand over property services to DATPOL One](#)
- [How to build a property maintenance plan](#)
- [How to report a fault so engineers can respond effectively](#)

11. Supply-point reconciliation and additional charges

The manager-only PPE tab compares imported or manually entered electricity consumption for a supply point with selected submeters for the same reading boundaries. Use imported energy in kWh, not power in kW or energy exported to the grid. Both boundary readings are required for every selected submeter.

An automatic Energa account connection has not been commissioned. Use the Mój Licznik portal or an invoice to obtain verified data. The current CSV import accepts the Podlicznik format: `ppe;start;end;kwh` and one period-total row. Dates use YYYY-MM-DD; the decimal separator may be a dot or comma. This does not claim compatibility with every operator export. Do not provide your Energa password in Podlicznik.

The difference in kWh and percentage is shown against a configurable threshold. A result within the threshold is not proof that an installation is correct. Investigate shared loads, losses, missing meters and mismatched periods. The residual is never automatically charged to tenants.

Additional net invoice charges can optionally be allocated by measured consumption or equally per selected point. Exclude charges already contained in the energy rate. Proportional allocation is blocked when consumption totals zero; rounding preserves the source total to the penny. Saved reconciliation is a separate CSV-exportable working statement, not a tax invoice, and does not trigger an email or tenant charge. Overlapping periods for the same PPE are rejected. These are Polish supply-point workflows; they do not assert compliance with UK energy billing rules.

[Energa-Operator data access information \(Polish\)](#)

12. Measurements from SNUT.pl

The intended flow is meter ? SNUT.pl ? Podlicznik. API connectivity is prepared and verified. The new device has not been added yet; existing devices from other properties have not been assigned to Podlicznik.

After commissioning in SNUT, provide DATPOL with the sensor entity, organisation and premises. The source must represent cumulative imported energy, not power, exported energy, PV generation or a daily-reset counter. DATPOL verifies the mapping and enables polling every five minutes. A serial number alone does not establish this mapping.

The portal shows the latest kWh register, Polish local timestamp and increase over available samples. Organisation and tenancy restrictions apply. Stale or unavailable data is not treated as zero. Decreases and source changes are quarantined for review. Telemetry does not automatically create billing-boundary readings; sampling and boundary validation will be agreed for the actual device. Historical backfill has not been commissioned.

13. Monthly PDFs at 00:01 and after-hours alerts

Managers enable delivery after checking recipients and rates. Processing starts on the first day of each month at 00:01 Europe/Warsaw, including daylight-saving changes. Actual arrival also depends on SMTP and the recipient mailbox. Tenants receive a branded PDF and managers receive a copy. It is not a tax invoice.

The PDF contains premises, meter identity, opening/closing registers, consumption, net amount and comparisons against each of the previous two months. Percentage change is $(\text{current} - \text{previous}) / \text{previous} \times 100\%$. Missing data and a zero denominator are clearly labelled. Other tenants' history is excluded. The same documents and comparisons are available in the portal, including direct PDF download.

Missing boundaries produce an incomplete report without a charge. The system uses approved dated registers or SNUT observations within the minute before midnight, without interpolation, and records the source. Incomplete reports require reviewed correction; there is no silent automatic replacement. No fictional premises are configured for delivery.

Alerts require an enabled per-meter rule: premises profile, weekly hours, permitted continuous load, excess kW, duration and cooldown. The suggested form values (0.3 kW above baseline for 15 minutes, six-hour cooldown) require property-specific confirmation. Refrigeration and servers need a realistic baseline. Detection uses consecutive cumulative-energy differences and at least three fresh readings outside business hours; overnight shifts are supported. Gaps, resets and stale values do not create false consumption spikes. A brief impulse is not equivalent to sustained demand. Alerts email the assigned tenant and appear in the portal; they are a prompt to investigate, not proof of a fault or intrusion.

Period-close checklist

1. Assign meter serial numbers to premises and tenants, with occupancy start and end dates.
2. Confirm opening and closing readings, units, transformer ratios and a common time boundary.
3. Distinguish actual readings, estimates and missing data. Never treat missing readings as zero.
4. Compare submeters with the main meter for the same period; investigate communal loads and differences.
5. Check rates, shared costs and the allocation method against the agreement; approve the statement.
6. Retain the report and corrections. Meter data supports charging; the applicable agreement and requirements determine the charging method.

Example: investigate a balance difference

The main meter records 1,200 kWh, two premises use 400 and 500 kWh, and communal loads use 200 kWh. The remaining 100 kWh needs investigation. Check periods, ratios, circuit boundaries, losses and gaps. Do not automatically charge the difference to one tenant. These are illustrative figures.

Podlicznik or Opomiarowani?

Podlicznik focuses on submetering and information for cost allocation. Opomiarowani extends this to environmental conditions, alerts and EMS. These scopes can be combined while keeping settlement readings, estimated costs and control separate. Metering, reporting and integration scope is confirmed before quotation.

Choose your next guide

- [Opomiarowani — sensors, alerts and measurement history explained](#)
- [EMS for local authorities — energy across schools, offices and municipal sites](#)
- [EMS for businesses — from consumption profiles to an improvement plan](#)
- [EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation](#)

Plan your installation with DATPOL

[View the service and implementation scope](#) · biuro@datpol.com · [+48 55 621 29 29](tel:+48556212929)

Updated 13 October 2026. Features are agreed for each installation.

EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation

[Czytaj po polsku](#)

EMS in practice: from measurements to informed decisions. A guide for property managers, businesses, municipalities and technical teams. It explains Energy Monitoring System design, data interpretation and integration with PV, storage and automation. This describes deployment options and principles; it does not imply that every control function is already commissioned at a customer site.

[Explore EMS from Opomiarowani by DATPOL](#)

Contents

1. [What is an EMS and how does it change daily work?](#)
2. [Who benefits: from individual premises to industrial and municipal sites](#)
3. [What we measure: kW is not kWh](#)
4. [Solar PV: see how much generation stays on site](#)
5. [Battery storage: more than charging at the lowest price](#)
6. [Dynamic prices: evaluate the whole decision](#)
7. [Demand peaks, contracted capacity and reactive energy](#)
8. [Hydrogen: monitoring the conversion chain](#)
9. [Architecture: from meter to a trustworthy report](#)
10. [Alerts, cybersecurity and control governance](#)
11. [Where monitoring supports obligations and audits](#)
12. [Specialist installations and billing need appropriate equipment](#)
13. [How to evaluate savings realistically](#)

1. What is an EMS and how does it change daily work?

An Energy Monitoring System collects data about consumption, generation and energy flows. Instead of reviewing bills, inverter applications and meter readings separately, you gain a shared view of the site.

Opomiarowani scopes range from readings and reports to agreed automation integration. Energy Management System describes wider management, potentially including control rules. Control functions are commissioned separately after equipment, process constraints and permissions have been checked. This service describes deployment options, not an identical feature set available at every site.

2. Who benefits: from individual premises to industrial and municipal sites

The greatest value comes when data informs an available decision. A factory can assess energy per shift or unit produced. A water utility can compare kWh per cubic metre pumped. Hotels can relate use to occupancy, and office managers to opening hours. Cold stores, farms and shops can analyse continuously operating equipment. Municipalities can compare schools, offices, sports facilities and lighting. Access is scoped to responsibilities; tenant energy statements can be linked with Podlicznik.

3. What we measure: kW is not kWh

kW describes instantaneous or interval-average power; kWh is energy used over time. We record import and export, active power and, with suitable analysers, reactive and apparent power, power factor, voltage, current and phase parameters. Data helps identify demand peaks, imbalance and deviations to investigate. Power-quality analysis, such as harmonics, requires appropriate instruments and recording settings. A basic kWh meter cannot

replace a power-quality analyser. Gas, heat, water and environmental readings can extend the picture.

4. Solar PV: see how much generation stays on site

PV generation alone does not show the full benefit. Inverter data is combined with supply-point and load measurements to separate on-site use, import and export. Self-consumption measures how much generation is used locally; self-sufficiency measures how much demand is met locally. With storage, flow directions must be considered to prevent double counting. Reports can identify loads suitable for moving into production periods, such as vehicle charging, hot-water preparation or permitted process cycles. Process reserves and user comfort remain overriding constraints.

5. Battery storage: more than charging at the lowest price

Depending on BMS and inverter interfaces, we analyse state of charge, available power, energy flows, temperature and limitation signals. A strategy may combine greater self-consumption, reduced demand peaks and a backup reserve. Nominal and usable capacity must be distinguished, with efficiency, charging power, SOC limits and warranty conditions included. An EMS cannot create backup capability if the electrical arrangement and inverter do not provide it. Control commands must respect the BMS, manufacturer protections and critical-load priorities.

6. Dynamic prices: evaluate the whole decision

The market price is only one part of the calculation. We assess the actual contract formula, supplier margin, variable charges, export rules and settlement intervals. Storage adds losses and battery wear costs. A negative market price does not automatically mean a negative bill. Planning may use PV and load forecasts and available prices, but forecasts remain distinct from measurements. Automatic load shifting or charging requires accessible interfaces, approved rules and defined behaviour when prices or connectivity are unavailable. Without control, the

system can still provide recommendations and scenario comparisons.

7. Demand peaks, contracted capacity and reactive energy

Simultaneous starts of large loads can create a peak hidden in monthly kWh totals. We analyse load over the intervals relevant to the contract and identify possible equipment sequencing. Peak reduction is useful where the process, storage and billing arrangements allow it. Reactive-energy recording helps assess charges and the need for a compensation study. An EMS does not itself compensate reactive power. Compensation equipment requires assessment of loads, harmonics and installation conditions. Not every instantaneous rise creates a billable exceedance.

8. Hydrogen: monitoring the conversion chain

A hydrogen project benefits from comparing electrolyser input, auxiliaries and compressor use, hydrogen production and energy recovered through a fuel cell. kWh/kg, operating time, availability and conversion losses can be assessed where the installation exposes suitable data. Tank pressure alone is insufficient for an accurate inventory without a model accounting for temperature and gas properties. Hydrogen integration is individually scoped with the designer and technology supplier. An EMS may receive status signals but does not replace hydrogen detection, ventilation, safety interlocks or safety controllers.

9. Architecture: from meter to a trustworthy report

Compatible sources are connected through Modbus RTU/TCP, pulses, documented APIs and MQTT. LoRaWAN can support periodic readings from dispersed points; it is not the basis for fast control loops or safety functions. Each point needs units, scaling, flow direction, timestamps and quality information. Cumulative kWh readings are differenced over time; power is integrated only with adequate sample quality. Meter replacement, resets, gaps and delayed data must be handled. Local buffering and history recovery depend on equipment and the agreed

10. Alerts, cybersecurity and control governance

Useful rules include after-hours consumption, communication loss, reversed energy flow, balance deviations and equipment limitations. Thresholds, delays and recipients follow the process. Integration starts with read access; writes require separate permissions, an allowed-command list and acceptance tests. Design can include OT/IT segmentation, encrypted channels, action logs, least privilege and update procedures. Cloud failure must not remove local protection. Public access to inverter or BMS control registers is not part of the design.

11. Where monitoring supports obligations and audits

There is no universal requirement for every business with PV to buy an EMS. Duties depend on the organisation, energy use, property and project conditions. Measurements support energy audits and investment evaluation. ISO 50001 also covers responsibilities, objectives and improvement; a dashboard does not establish certification. Article 11 of EU Directive 2023/1791 distinguishes above 85 TJ for an energy management system and above 10 TJ for audits, using three-year average annual consumption across all energy carriers. These are EU-level provisions; applicability, deadlines and Polish implementing law require organisation-specific checking. This English version describes the Polish service context, not UK compliance. Sources appear below.

12. Specialist installations and billing need appropriate equipment

Hydrogen requires a separate hazard assessment, suitable equipment for classified areas and review of pressure-equipment and inspection requirements. A process-system reading does not replace required protections. Likewise, energy monitoring does not replace the operator's settlement meter; billing use requires

checking applicable metrological requirements. Connection conditions, export limits, funding terms or contracts may impose further recording duties. The proposal distinguishes operational indications from measurements intended for documentation or settlement.

13. How to evaluate savings realistically

First establish a baseline: use, cost, working hours, production, weather and site changes. After deployment, compare equivalent conditions rather than merely two bills. Lower kWh may reflect reduced production rather than improved efficiency. Assess integration and support costs, storage losses and equipment life. Useful indicators include kWh/m², kWh per production unit, period cost, overnight demand and the local-energy share. An EMS helps identify and measure improvements; it does not guarantee a savings percentage without data analysis.

14. Phased deployment: measurement, decisions, automation

1. Inventory meters, PV, storage, tariffs and loads. 2. Design measurement points and secure communication. 3. Commission readings and compare them with equipment. 4. Establish a baseline, indicators and alerts. 5. Evaluate operational changes and their economics. 6. Add optional control after agreeing priorities, limits and tests. 7. Review outcomes and maintain the system. For an initial discussion, provide bills and a load profile, inverter and storage models, an installation diagram and working hours. DATPOL will scope integration and quote for the particular site.

15. Terms and basic calculations

Quantity	Meaning	Check
kW / kWh	Power / energy over time.	Do not compare instantaneous power with monthly consumption.

Quantity	Meaning	Check
kvar / kvarh	Reactive power / reactive energy.	Check direction, signs and contractual charges.
SOC / SOH	State of charge / estimated battery health.	SOH depends on the manufacturer's method; it is not a direct remaining-runtime measurement.
PPE	Polish supply-point identifier.	The measurement boundary must match the meters included in reconciliation.
Self-consumption	Share of local generation used on site.	Distinguish direct use from energy passing through storage.
Self-sufficiency	Share of demand met locally.	This uses a different denominator from self-consumption.
Round-trip efficiency	Energy discharged / energy charged.	Use the same AC or DC boundary and account for auxiliaries.

Example without storage: PV generates 100 kWh, with 60 kWh used locally and 40 kWh exported. Self-consumption is 60%. If total site demand is 150 kWh, self-sufficiency is 40%. Zero generation or demand makes the corresponding percentage undefined; do not divide by zero.

Energy increment: closing minus opening register, with the verified ratio and unit applied. A falling cumulative register needs reset or replacement checks. A constant 10 kW over 30 minutes represents 5 kWh. Variable power requires integration or properly sampled data.

16. Storage economics example

Illustrative assumptions: purchase 100 kWh at a full variable import cost of PLN 0.40/kWh; at 90% round-trip efficiency, use the discharged 90 kWh instead of imports at PLN 0.90/kWh. Avoided expenditure is PLN 81 and charging cost PLN 40. Deduct an illustrative PLN 5 wear allowance: the cycle contribution is PLN 36. Investment, fixed charges and taxes are excluded. This is not a price forecast or a return guarantee. Where the energy could have been sold, include the opportunity cost of forgone exports.

17. What should each measurement point contain?

- Unique identifier, site, circuit and organisation assignment.
- Device model, register/protocol, unit, multiplier and flow direction.
- Measurement and receipt timestamps, time zone and daylight-saving handling.
- Quality status: valid, stale, missing, estimated or error.

- Raw and converted values and configuration-change history.
- Retention, export, backup and access rules; personal data should not appear in public identifiers.

Do not add the main meter and its submeters as separate costs for the same property. Align period boundaries and check completeness before comparing data. Inverter power, meter energy and model forecasts are different data types.

18. Commissioning checklist

1. Compare system values with the device; verify scaling, signs and units.
2. Confirm balance topology, assignments and absence of double counting.
3. Check timestamps, gaps, meter resets and reconnection under controlled conditions.
4. Test an alert and confirm recipient, threshold, delay and message rate limits.
5. Check account isolation and export of only the correct organisation's data.
6. Compare the first report with readings and relevant invoice components.
7. Where control is included, accept it separately: limits, priorities, manual override and connectivity loss.
Tests must not impair process protection.
8. Record responsibilities, contacts, change procedures and maintenance plans.

19. Common issues and initial checks

Symptom	Check
Consumption is several times too high.	W versus kW, Wh versus kWh, transformer ratios and duplicate scaling.
The balance does not reconcile.	Time boundaries, common areas, flow directions, missing points and storage.
The chart shows zero after a fault.	Whether missing data was incorrectly converted to zero.
Storage differs from the plan.	BMS limits, SOC reserve, inverter schedules, temperature and write permissions.
Cost differs from the invoice.	Net/gross, fixed charges, distribution, period, rates and data completeness.
Too many alerts.	Process profile, hysteresis, exceedance duration, aggregation and recipients.

Do not change BMS protection, protective settings or wiring to make a result fit. Report the device model, measurement point, event time and expected result. Never send passwords or tokens.

20. Questions and answers

Does an EMS automatically control every battery?

No. It requires a compatible interface, control authorisation and a design respecting the BMS, warranty and installation limits. Monitoring can be the first stage.

Do dynamic prices always reduce the bill?

No. Results depend on the load profile, contract, charges and ability to shift demand. An EMS allows scenarios to be compared using data.

Can equipment from different manufacturers be integrated?

We assess models, protocols, data access and permissions. Integration is confirmed after checking, separately for reading and control.

21. Sources and currency

References checked on 6 October 2026. At deployment, review current legislation, amendments, contracts and equipment documentation. This guide does not replace a site-specific assessment.

- [URE — dynamic-price contracts](#)
- [EUR-Lex — Energy Efficiency Directive, Article 11](#)
- [Polish Energy Efficiency Act — consolidated text](#)
- [ISO 50001 — energy management](#)
- [UDT — hydrogen storage and tanks](#)

Related guides

- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)
- [What to prepare before connecting a public authority to a SOC](#)
- [How to prepare a business for an audit without disrupting operations](#)

Choose your next guide

- [Opomiarowani — sensors, alerts and measurement history explained](#)
- [EMS for local authorities — energy across schools, offices and municipal sites](#)
- [EMS for businesses — from consumption profiles to an improvement plan](#)
- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)

Plan your installation with DATPOL

[View the service and implementation scope](#) · biuro@datpol.com · [+48 55 621 29 29](tel:+48556212929)

Updated 13 October 2026. Features are agreed for each installation.

Opomiarowani — sensors, alerts and measurement history explained

[Czytaj po polsku](#)

Choose measurement points, define alerts and accept an installation. Temperature, humidity, utilities and DATPOL Control.

What does Opomiarowani provide?

Opomiarowani is a DATPOL service covering the selection, installation and integration of measurements, with an agreed support scope. Users can view selected sites together instead of checking individual device displays.

DATPOL Control provides the interface; available information depends on the equipment and integrations commissioned.

Start with one warehouse, refrigerator or distribution board, then expand. First define the question: are conditions acceptable, where is energy used, is equipment running, and who should respond?

Choose measurements around the problem

- **Warehouses and archives:** temperature, humidity, excursions and their duration.
- **Cold rooms and refrigerators:** representative measurement locations, history and limits appropriate to the stored product.

- **Server rooms:** conditions around racks, water leaks, cooling availability and UPS signals where supported.
- **Energy and utilities:** meter readings, consumption profiles and unexpected demand.

One temperature limit does not suit every product. Define range, accuracy, location and calibration needs before choosing sensors.

How does information reach the dashboard?

Sensors and meters communicate over wired or wireless links, such as Modbus or LoRaWAN. A gateway transports information to the system. We check coverage, power, network access and behaviour during communication outages. LoRaWAN is primarily used for periodic measurements; reporting intervals depend on the application and sensor power source.

The reading and its timestamp both matter. Missing information is a separate condition, not evidence that conditions are normal. Retention, reports and any backfilling after an outage form part of the agreed scope.

Alert, recipient and response

1. Set the threshold, delay and return-to-normal condition.
2. Identify recipients and duty hours; agree SMS, email or another supported channel.
3. Define escalation and who acknowledges the incident.
4. Test an excursion, lost communications and restored data.

A notification does not repair equipment. Assign an action and an owner. Control requires a separate agreement covering permissions, feedback and local operation when internet access is lost.

Acceptance and everyday operation

- Compare measurements against a reference and check units and time zones.
- Verify site assignment, labels, sensor location and user access.

- Test charts, date selection, reports and missing-sample indications.
- Agree battery replacement, maintenance, calibration and incident handling.

For a quotation, provide the number of sites and measurements, environmental conditions, required accuracy, existing device models and internet availability. Do not send passwords with an enquiry.

Choose your next guide

- [EMS for local authorities — energy across schools, offices and municipal sites](#)
- [EMS for businesses — from consumption profiles to an improvement plan](#)
- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)
- [EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation](#)

Plan your installation with DATPOL

[View the service and implementation scope](#) · biuro@datpol.com · [+48 55 621 29 29](tel:+48556212929)

Updated 13 October 2026. Features are agreed for each installation.

EMS for local authorities — energy across schools, offices and municipal sites

[Czytaj po polsku](#)

A practical plan for local authorities: measurement points, site responsibilities, building comparisons, reports and a pilot.

One view across public organisations

A local authority needs a portfolio overview, while a school manager needs information about their own building. An EMS design combines shared site and supply-point naming, measurements and access scopes. The aim is to identify causes of consumption and actions whose effects can subsequently be checked.

Group sites by function: schools, nurseries, offices, sports facilities, treatment plants and other municipal buildings. A raw kWh ranking is not an efficiency ranking: floor areas, operating hours and processes differ.

Where should measurement start?

Area	What to observe	Example decision
Schools and offices	Out-of-hours and weekend demand; heating and ventilation profiles	Review operating schedules
Sports facilities	Lighting and HVAC against occupancy	Match operating hours to use

Area	What to observe	Example decision
Municipal processes	Energy against running time and process output	Assess pumps or compressors
PV and storage	Generation, import, export and storage state	Assess self-consumption and control scenarios

Information, responsibilities and reports

- **Energy coordinator:** portfolio review, exceptions and action planning.
- **Site manager:** their building, local alerts and explanations.
- **Technical team:** communications, equipment health and agreed interventions.

Agree monthly reporting: consumption, costs under the agreed model, missing information, out-of-hours demand and actions with owners. Compare kWh/m² only across suitable functions and periods, allowing for weather and changes in use.

Prepare a pilot and procurement scope

1. Select representative buildings and gather bills, supply-point details, tariffs and operating hours.
2. Inventory meters, boards, PV and interfaces; identify where submeters are needed.
3. Define data intervals, retention, export, access roles, support and data ownership.
4. Commission readings, compare them with the meter and flag incomplete periods.
5. Establish the baseline and select actions. Seasonal conclusions require suitable historical coverage.
6. Expand once data quality and usefulness have been demonstrated.

Control and verification of outcomes

Monitoring can be commissioned before automation. Changes to heating, ventilation or lighting schedules must account for comfort, building use and local protection. Storage needs a compatible inverter, a confirmed interface and operating limits. A visible reading alone does not authorise control.

The system supports energy management practices and evidence-based decisions. Buying a dashboard does not constitute ISO 50001 certification or fulfil every public-sector obligation. Organisational and legal requirements are assessed separately. No savings percentage is promised without comparison data. This guide concerns Polish local authority projects; the English version does not establish UK compliance.

[ISO 50001 — energy management context](#)

Choose your next guide

- [Opomiarowani — sensors, alerts and measurement history explained](#)
- [EMS for businesses — from consumption profiles to an improvement plan](#)
- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)
- [EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation](#)

Plan your installation with DATPOL

[View the service and implementation scope](#) · biuro@datpol.com · [+48 55 621 29 29](tel:+48556212929)

Updated 13 October 2026. Features are agreed for each installation.

EMS for businesses — from consumption profiles to an improvement plan

[Czytaj po polsku](#)

Process submetering, overnight demand, tariffs, PV and storage. Metrics, input data and commissioning checks.

Measure what you can influence

A business EMS should identify which sites, processes and operating periods drive consumption. The main meter shows the overall balance, while submeters separate production, cooling, compressed air, storage areas, offices and tenants. We design around decisions rather than the number of charts.

Start by asking: what runs after work ends, when does demand peak, what changed after a machine was installed, and how much locally generated energy is used on site?

Five views worth defining

1. **Site balance:** imported energy, PV generation, export and storage, with defined measurement boundaries.
2. **Loads and processes:** compare departments without double-counting the main meter and its submeters.
3. **Time profile:** shifts, shutdowns, nights and weekends.
4. **Cost:** an estimate based on the contract and tariff, clearly separate from the supplier invoice.
5. **Data quality:** latest reading, missing samples, transformer ratios and communication status.

Metrics for processes and buildings

kWh per item, tonne or operating hour requires reliable production quantities for the same period. Building analysis can use kWh/m² and out-of-hours demand. Lower production can reduce total consumption while making unit efficiency worse.

Illustrative calculation: an unnecessary constant 3 kW load for 12 hours a day over 22 days uses 792 kWh. Estimate the cost using the applicable rate and contract components. This is an example, not a measured customer result or a savings guarantee.

Tariffs, solar PV and storage

We distinguish the distribution network operator from the energy supplier. Purchase cost depends on the contract; the wholesale price alone is not the full cost of a kWh. Dynamic tariff analysis needs the relevant settlement periods, margins and distribution components, with correct time zones and daylight-saving treatment.

Battery scenarios require power and capacity, permitted state of charge, efficiency, reserve and import/export limits. We start with simulation. Automatic control requires confirmed compatibility and acceptance testing, including local protection and warranty conditions.

Implementation and acceptance

1. Gather bills, consumption profiles, operating hours and meter, inverter and storage models.
2. Define the measurement hierarchy, labels, units, transformer ratios and user access.
3. Commission readings and verify energy direction, timestamps and device agreement.
4. Define metrics, alerts and action owners.
5. Check period reports, gaps and export.
6. Compare outcomes under similar production and operating conditions.

The quotation separates equipment, installation, integration, reporting, optional automation and support. Data can support an ISO 50001 energy management system; the dashboard does not replace policies, targets, responsibilities or performance review. Regulatory assessment relates to the project location; British English is the language of this guide.

Choose your next guide

- [Opomiarowani — sensors, alerts and measurement history explained](#)
- [EMS for local authorities — energy across schools, offices and municipal sites](#)
- [Podlicznik — meter readings, tenant charges and reports: a property manager's guide](#)
- [EMS — Energy Monitoring System: measurements, solar PV, storage and cost optimisation](#)

Plan your installation with DATPOL

[View the service and implementation scope](#) · biuro@datpol.com · [+48 55 621 29 29](tel:+48556212929)

Updated 13 October 2026. Features are agreed for each installation.