POWERSCREEN®
OF CALIFORNIA, NEVADA & HAWAII a Molson Group Company

Data Breach Policy & Procedures

Department: Marketing
Date of issue: 01/02/2025
Version: 1.1

Document Author: Jordan Fontaine
Last Updated: 01/02/2025

Table of Contents

Policy Statement

Powerscreen of California, Nevada, & Hawaii, an entity of Molson Group, (hereinafter referred to as "the Company," "we," "us," or "our") is committed to compliance with applicable privacy laws and regulations, including the **California Consumer Privacy Act (CCPA)**. We maintain a robust and structured program for compliance, monitoring, and risk management to protect personal information and mitigate risks associated with data breaches.

We perform regular risk assessments and audits to ensure our compliance processes, procedures, and controls are fit for purpose. Recognizing that breaches can still occur, this policy sets out our intent and objectives for managing such incidents.

Protecting the personal information of consumers, clients, and employees is of paramount importance, and we operate under a **Privacy by Design** approach to safeguard data. This policy works in conjunction with our Data Protection and Information Security Policies.

Purpose

The purpose of this policy is to define the Company's intent, objectives, and procedures for managing data breaches involving personal information. Under the **CCPA**, we are obligated to implement and maintain adequate measures to protect personal information and to provide mechanisms for identifying, reporting, and responding to data breaches. This policy ensures that all employees understand the protocols and reporting procedures for addressing data breaches and incidents.

Scope

This policy applies to all staff within the Company, including permanent, fixed-term, and temporary staff, third-party representatives or sub-contractors, agency workers, volunteers, interns, and agents engaged with the Company in the United States or internationally. Adherence to this policy is mandatory, and non-compliance may result in disciplinary action.

Data Security and Breach Requirements

The Company defines a data breach as any incident involving unauthorized access, destruction, loss, alteration, or disclosure of personal information. We have established robust technical and organizational measures to mitigate these risks, including but not limited to:

- **Encryption and Pseudonymization**: To protect sensitive personal information.
- **Access Controls**: Restricted access and biometric measures to prevent unauthorized access.
- **Incident Response Plans**: Procedures to restore the availability and access to personal information in the event of a breach.
- **Ongoing Training**: Regular training and assessments for employees on data protection and breach management.
- **Audit and Testing**: Regular audits and testing of security measures to ensure their effectiveness.
- **Data Disposal Protocols**: Procedures to ensure secure disposal of personal information.

We conduct frequent information audits and risk assessments to identify vulnerabilities and ensure compliance with the CCPA's requirements for protecting personal information.

Objectives

The Company's objectives for data security and breach management include:

1. **Compliance with the CCPA**: Ensuring all processes and procedures align with CCPA requirements.
2. **Risk Mitigation**: Utilizing risk assessments and information audits to minimize the risk of breaches.
3. **Breach Response**: Implementing clear protocols for identifying, investigating, and reporting breaches promptly.
4. **Consumer Protection**: Safeguarding the personal information and privacy rights of consumers, clients, and employees.
5. **Regulatory Notification**: Notifying affected parties and regulatory authorities in accordance with applicable timelines.
6. **Continuous Improvement**: Using breach logs and root cause analysis to prevent recurrence.

Data Breach Procedures and Guidelines

The Company has developed comprehensive procedures for managing data breaches, including:

1. **Breach Reporting**:
   - All breaches, regardless of severity, must be reported immediately to the **Data Protection Officer (DPO)** or designated personnel.
   - Employees are trained to recognize potential breaches and report incidents promptly.
2. **Investigation**:
   - Each reported breach is investigated to determine its cause, scope, and impact on personal information.
   - Investigations are documented in breach logs, which are analyzed for patterns and improvement opportunities.
3. **Containment and Mitigation**:
   - Steps are taken to contain the breach and mitigate any further risks, including isolating affected systems and securing compromised data.
   - Where necessary, changes to systems and processes are implemented to prevent recurrence.
4. **Consumer Notification**:
   - If a breach involves personal information of California residents, affected individuals are notified without unreasonable delay, as required by the **CCPA**.
   - Notifications include the nature of the breach, the type of information affected, and steps individuals can take to protect themselves.
5. **Regulatory Notification**:
   - If the breach meets notification thresholds under applicable laws, the Company will notify the appropriate regulatory bodies within the required timeframe.
6. **Documentation and Review**:
   - All breaches are recorded and analyzed to identify trends and areas for improvement.
   - The findings are used to update training, policies, and procedures to strengthen data protection.

Commitment to Consumer Privacy

The Company is committed to respecting and protecting consumer privacy rights under the CCPA. By implementing this policy, we ensure that personal information is safeguarded, and breaches are managed effectively to minimize their impact.

Breach Incident Procedures

Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the reporting officer Data Protection Officer immediately so that breach procedures can be initiated and followed without delay. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Company and is not about apportioning blame. These procedures are for the protection of the Company, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.
As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

Breach Recording

The Company use a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder (electronic or hard copy) and reviewed against existing records to ascertain patterns or reoccurrences. The Company use separate breach incident form templates for incidents relating to PECR and US GDPR breaches to ensure that the correct information is recorded and reported.
In the event of a data breach, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.
A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.
If applicable, the Commissioner and the data subject(s) are notified in accordance with the US GDPR and/or PECR requirements (refer to section 6 of this policy). The Commissioner protocols are to be followed and the ICO 'Security Breach Notification Form' should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.
A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Company's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.
Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas.
- Re-assessment of compliance knowledge and understanding.
- Suspension from compliance related tasks.
- Formal warning (in-line with the Company's disciplinary procedures).

System Error

- Where the data breach is the result of a system error/failure, the IT team will work in conjunction with the DPO to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.
- Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -
- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system.
- Removing an employee from their tasks.
- The use of back-ups to restore lost, damaged or stolen information.
- Making the building secure.
- If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed.

Assessment of Risk and Investigation

The DPO should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved.
- It's sensitivity or personal content.
- What protections are in place (e.g. encryption)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident.

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

Breach Notifications

The Company recognise its obligation and duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities. We have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported immediately.
In relation to US GDPR breaches, the Company recognise it is required to notify the Commissioner (and where applicable the data subject), where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.
Under the PECR and the US GDPR, the Commissioner is to be notified of any data breaches that meet certain criteria. The Company use dedicated GDPR and PECR Breach Incident Forms to ensure that all required information has been recorded and is notified to the ICO within the mandatory timeframes.

ICO Notification for PECR Breaches

Where the Company identify a personal data breach in relation to a service or technology defined by the PECR, we notify the Commissioner without undue delay. The Company use a PECR Data Breach Incident Form to record any breaches and actions.

The PECR breach notification to the Commissioner contains: -

- The nature of the personal data breach.
- The consequences of the breach.
- The measures taken or proposed to be taken by the provider to address the breach.

Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Commissioner if requested.

Subscriber or User Notification

Where a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or user, the Company also notify the person(s) concerned without undue delay. We ensure that all communications to users or subscribers are in a written, clear and legible format.

The notification to the subscriber or user shall include: -

- A description of the nature of the breach.
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact for obtaining further information.
- Recommendations of measures to allow the subscriber/user to mitigate the possible adverse impacts of the breach.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed by the Company to address the data breach.

We reserve the right not to inform the subscriber or user about the breach where we have demonstrated, to the satisfaction of the Information Commissioner, that: -

- the Company have implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it, and
- that those measures were applied to the data concerned in that breach.

The Company recognise that where it chooses not to notify the subscriber or user the Information Commissioner may, having considered the likely adverse effects of the breach, require us to do so. We retain detailed information of any personal data breaches to ensure that notifications can be made should they be required.

ICO Notification for US GDPR Breaches

The Company recognise its obligation to notify the Information Commissioner where any data breach is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.
Where applicable, the Commissioner is notified of the breach no later than 72 hours after the Company becomes aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.
If for any reason it is not possible to notify the Commissioner of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Commissioner in accordance with Article 33 of the US GDPR.
The notification to the Commissioner will contain:

- A description of the nature of the personal data breach.
- The categories and approximate number of data subjects affected.
- The categories and approximate number of personal data records concerned.
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information).
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).

Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Commissioner if requested.
Where the Company act in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.
The notification to the Data Subject shall include: -
The nature of the personal data breach.
The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information).
A description of the likely consequences of the personal data breach.
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).
We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.
If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Responsibilities

The Company ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.
The Data Protection Officer (if applicable) is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.