Valmont Privacy Policy ANZ

1.0 Definitions & Scope

Valmont Australia is committed to protecting the privacy of individuals' personal information and to complying with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), the Privacy Act 2020 (NZ), including the Information Privacy Principles (IPPs), and other applicable privacy, credit reporting and data protection requirements.

This policy sets out the privacy commitments of Valmont Australia Pty Ltd (ABN 58 000 507 415) and its Australian and New Zealand subsidiaries, controlled entities and business units from time to time, including Industrial Galvanizers Corporation Pty Ltd (including Valmont Coatings, Ingal Civil Products, Ingal EPS, Site Pro 1 and Valmont Utility); Galvline Tasmania Pty Ltd; Webforge Australia Pty Ltd; Locker Group Pty Ltd (Webforge Locker); Valmont Irrigation Australia Pty Ltd; H-R Products; Valmont Highway International Pty Ltd; Valmont (NZ) Group Ltd; Webforge (NZ) Ltd; Valmont Coatings (NZ) Ltd; Industrial Galvanizers Corporation (NZ) Ltd; Valmont Highway Technology Ltd; and Valmont Highway Distribution Ltd (together, the “Company”, “we”, “our” or “us”). The Company forms part of the global Valmont group. References in this policy to the “Valmont Group” mean Valmont Industries, Inc., its subsidiaries and other related bodies corporate worldwide.

This policy applies to personal information handled in connection with customers, prospective customers, suppliers, contractors, employees, applicants, guarantors, directors or officers of customer entities, and other workplace or business participants. It is intended to operate across the Company's Australian and New Zealand business units, subject to any additional or different requirement imposed by applicable law.

Personal information has the meaning given by applicable privacy law and generally means information or an opinion about an identified individual, or an individual who is reasonably identifiable. Sensitive information, credit information, credit eligibility information, tax file numbers and other regulated information are handled in accordance with any additional legal requirements that apply to those categories.

This policy explains the kinds of personal information the Company may collect and hold, why it is collected, how it may be used and disclosed, how it is protected, and how an individual may request access or correction or make a privacy complaint. Specific collection notices, credit application notices or consent statements may supplement this policy where required for a particular transaction or business process.

Nothing in this policy is intended to create contractual rights or obligations beyond those imposed by applicable law, or to limit any right, exemption, defence or permission available to the Company under applicable law.

2.0 Collection of Personal Information

The Company will collect personal information where it is reasonably necessary for its functions or activities, including conducting its business, providing products or services, administering commercial relationships, assessing or managing credit, and meeting employer or legal obligations.

Personal information may be collected directly from an individual through communications with us, websites, forms, credit applications, employment records or other dealings. It may also be collected from

third parties or publicly available sources where permitted by law, including related Valmont Group entities, referees, trade references, credit reporting bodies, identity verification providers, insurers, professional advisers, government or regulatory bodies, and service providers.

Depending on the dealings involved, information collected and held may include names and contact details; identity and business role details; employment history, qualifications, remuneration, benefits and tax or banking details; health and safety information; financial and credit-related information; and correspondence, transaction records and website or system activity.

The Company will take reasonable steps to provide notices required by applicable privacy laws. Where personal information is collected indirectly in New Zealand, the Company will comply with IPP 3A of the Privacy Act 2020, to the extent applicable and subject to any statutory exceptions.

The Company will only collect sensitive information where permitted by law, including where the individual has consented and whether the information is reasonably necessary for the Company's functions or activities, or where another legal exception applies. Tax File Numbers and other government-related identifiers are not treated as ordinary identifiers and will be collected, used and disclosed only as permitted by applicable law.

Where the Company is required or authorised by law to collect personal information, it will take reasonable steps to inform the individual of the relevant requirement or authority where the applicable privacy law requires this.

3.0 Use of Personal Information

The Company may use personal information where reasonably necessary for its functions and activities, including:

- providing customers with products, services and customer support;
- communicating with customers and prospective customers about products, services and account matters;
- communicating with suppliers, contractors and other business partners;
- assessing credit applications, creditworthiness, guarantees and trading terms, managing credit accounts, collecting debts, preventing fraud and managing commercial risk;
- managing employees, contractors and other workplace participants, including compliance with employment obligations, remuneration, share plans and employee benefits;
- supporting the health, safety and welfare of workplace participants when performing work for the Company;
- obtaining and administering appropriate insurance coverage;
- meeting Australian and New Zealand taxation, superannuation/KiwiSaver and other legal or regulatory obligations; and
- establishing, exercising or defending legal or equitable claims and investigating suspected unlawful activity or serious misconduct.

Where the Company uses personal information for direct marketing, it will do so only where permitted by applicable law. In Australia, individuals will be provided with a simple means to opt out of direct marketing and the Company will comply with an opt-out request. Electronic marketing will also be conducted in accordance with applicable anti-spam laws.

4.0 Disclosure of Personal Information

The Company may disclose personal information in confidence to related Valmont Group entities, contractors, subcontractors, professional advisers and service providers where reasonably necessary for the Company's business or the purposes described in this policy. The Company may also disclose information in connection with joint promotions, financing, insurance, credit assessment, debt recovery, fraud prevention, legal compliance or business administration. Where appropriate, the Company will require third parties handling personal information on its behalf to protect it consistently with applicable law and contractual requirements.

Personal information may be disclosed to a potential purchaser, investor or successor in connection with a proposed or actual sale, merger, restructuring or transfer of all or part of the Company's assets or business, subject to appropriate confidentiality safeguards.

The Company will not sell personal information to third parties for the purpose of enabling those third parties to market their own products or services to the individual.

Otherwise, the Company will use or disclose personal information for the purpose for which it was collected, or for a permitted secondary purpose, including where the individual has consented, the individual would reasonably expect the use or disclosure and the law permits it, or the use or disclosure is required or authorised by law or a court or tribunal order.

The Company may also use or disclose personal information where a permitted general situation or comparable legal exception applies, including to lessen or prevent a serious threat to life, health or safety, to investigate or remedy suspected unlawful activity or serious misconduct, for the establishment, exercise or defence of a legal or equitable claim, or for proceedings before a court or tribunal or implementation of its orders.

5.0 Credit Applications and Credit Reporting

Where a Valmont business unit provides, considers providing, or manages credit and applicable credit reporting laws apply, the Company may collect, hold, use and disclose personal information and credit-related information about individuals associated with a credit application or account, such as sole traders, directors, officers, guarantors or other relevant individuals.

For Australian credit applications, where the relevant Valmont entity is a credit provider for the purposes of Part IIIA of the Privacy Act 1988 (Cth), the Company will comply with the additional requirements applying to credit providers and any binding Privacy (Credit Reporting) Code. This may include giving required notices before disclosing personal information to a credit reporting body and maintaining any required credit reporting policy.

The Company may exchange permitted information with any credit reporting agencies / bodies including but not limited to Equifax, Dun & Bradstreet etc., and with trade referees, debt collection agencies, insurers and other permitted recipients for purposes such as assessing an application for credit, verifying identity and information supplied, assessing creditworthiness and commercial risk, managing an account, recovering amounts owing, preventing fraud and complying with legal obligations.

Where required by Australian credit reporting law, a collection notice or credit application will identify the relevant credit reporting body and its contact details and will explain applicable rights relating to access, correction, complaints and credit-reporting information. This policy does not replace any transaction-specific notice or consent required by law.

6.0 Automated Credit Assessment and Decisions

The Company may use automated systems, computer programs, artificial intelligence (AI), machine learning tools, scoring models and other technology-assisted processes when assessing applications for commercial credit, trade accounts, finance facilities, guarantees, or related credit products, and to manage credit relationships in Australia and New Zealand.

These systems may be operated by the Company or by providers acting on its behalf.

Information used

The kinds of personal information that may be used by these automated systems include:

- Identity and contact information;
- Director, shareholder, trustee, partner, guarantor and beneficial owner information;
- Identification and verification information;
- Credit history and credit-related information;
- Financial and banking information;
- Business trading history and account conduct information;
- Information obtained from credit reporting bodies, commercial credit bureaus and fraud prevention agencies;
- Information provided in connection with your application; and
- Information collected from publicly available sources where permitted by law.

Decisions made or assisted by automated systems

The Company may use these systems to assist with, or in some circumstances, to make decisions by automated means about:

- Credit application approvals or declines;
- Creditworthiness and risk assessments;
- Credit limit recommendations or allocations;
- Ongoing account reviews and monitoring;
- Fraud prevention and identity verification;
- Compliance and anti-money laundering checks;
- Account management decisions; and
- Collection and recovery activities.

This includes decisions where an automated assessment is a substantial basis for a staff member's final decision. For example, automated systems may be used to generate risk scores, recommendations, alerts, classifications or other outputs that are substantially and directly related to a credit decision. These outputs may be relied upon by our personnel when making decisions regarding a credit application or ongoing credit relationship.

Where appropriate, we may use automated systems to make certain decisions without direct human involvement. We maintain appropriate governance, oversight and review processes designed to support fair, accurate and lawful decision-making.

These decisions can affect whether credit is offered, the amount and terms of credit, continued access to an account, and recovery of outstanding amounts.

7.0 Overseas and Cross-Border Disclosures

Because the Company is part of the global Valmont Group and uses external service providers, personal information may be disclosed to recipients located outside Australia or New Zealand where reasonably necessary for the purposes described in this policy.

Where Australian privacy law applies, before disclosing personal information to an overseas recipient the Company will take reasonable steps required by APP 8 to ensure that the recipient does not breach the APPs in relation to the information, unless an applicable exception applies. The countries in which overseas recipients are likely to be located are: Malaysia and United States of America.

Where New Zealand's IPP 12 applies, the Company will ensure that an applicable legal basis for the disclosure exists, including by establishing comparable safeguards where required, or obtaining informed authorisation where the Act permits that approach.

The Company distinguishes between a disclosure to another entity and the use of a service provider acting solely as the Company's agent for storage or processing where applicable law treats those arrangements differently.

8.0 Security, Retention and Data Breaches

The Company may be required by law or legitimate business needs to retain certain personal records for specified periods after the last transaction, employment event or other relevant activity.

The Company will take reasonable steps, including appropriate technical and organisational measures, to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Measures may include access controls, security procedures, staff training, contractual controls over service providers, system monitoring and other safeguards appropriate to the nature and sensitivity of the information and the relevant risks.

Where personal information is no longer required for a permitted purpose and the Company is not required by law or a court or tribunal order to retain it, the Company will take reasonable steps to destroy it or ensure it is de-identified, as applicable.

The Company maintains processes to identify, contain, assess and respond to actual or suspected privacy or data breaches. Where a breach is notifiable under applicable law, including Australia's Notifiable Data Breaches scheme or the New Zealand Privacy Act 2020, the Company will notify the relevant regulator and affected individuals as required by law.

9.0 Access to, and Correction of, Personal Information

The Company will take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up to date, complete and, where relevant, appropriate for the purpose for which it is used or disclosed.

An individual may request access to personal information held by the Company about them, or request correction where they believe information is inaccurate, out of date, incomplete, irrelevant or misleading. The Company may need to verify identity before providing access or making a correction.

The Company will respond to access and correction requests in accordance with applicable law. Access may be refused or limited where the law permits or requires this, in which case the Company will provide any notice or reasons required by law and information about applicable complaint rights.

Where Australian credit reporting law applies, additional access and correction rights and procedures may apply to credit information and credit eligibility information.

10.0 Technology and Privacy

Individuals interacting or transacting with the Company should be aware that software used to operate networks, websites, mail servers, gateways and other systems may create logs of transactions, communications and system activity.

Such logs may include email addresses of senders and recipients, dates and times of transmission, device or network information and website activity. The content of emails is not ordinarily logged by network software but may be stored on mail servers and may be accessible to authorised Company system administrators where required for legitimate operational, security, legal or compliance purposes.

The Company cannot guarantee that recipients outside the Company will apply the same privacy practices to communications or information sent to them. Personal information contained in Company email, internet or other systems remains subject to this policy and applicable law while held by the Company.

Employees using Company email, internet and technology services should also comply with the Company's applicable systems usage, information security and technology policies.

11.0 Privacy Enquiries and Complaints

An individual who has a question, access or correction request, or complaint about the Company's handling of personal information should first contact the relevant Valmont business unit or the Company's designated Privacy Officer/privacy contact. The Company will assess and respond to privacy complaints within a reasonable period and in accordance with applicable law.

A complaint should provide sufficient details to allow the Company to understand and investigate the issue. The Company may request further information where reasonably necessary to investigate or resolve the matter.

If an individual is not satisfied with the Company's response, they may have the right to contact the Office of the Australian Information Commissioner (OAIC) in Australia or the Office of the Privacy Commissioner in New Zealand.

12.0 Changes to this Policy

The Company may revise this policy from time to time to reflect changes in law, technology, business practices or the Company's operations. The current version will be made available electronically or through other appropriate channels.

The Company's handling of personal information will be governed by the policy and applicable law in effect at the relevant time. Where a material change requires additional notice or consent under applicable law, the Company will take the steps required by that law.

13.0 Further Information and Regulatory Contacts

Valmont Privacy Contact:

Mike Spry - Strategic People Partner

Michael.Spry@valmont.com

Contact Number : +61(7)31854891

Australia - Office of the Australian Information Commissioner (OAIC)

Telephone: 1300 363 992

www.oaic.gov.au

New Zealand - Office of the Privacy Commissioner

Telephone: 0800 803 909

www.privacy.org.nz

Authorisation

This revised policy is to be reviewed and approved by the appropriate Valmont Australia & New Zealand authorised officer before publication or operational use.

Mike Spry
Strategic People Partner

Policy Version History

Version	Date	Summary of Key Changes
1.0	17/04/2014	Initial Policy Release
1.1	18/01/2016	Updating Definitions and Scope
1.2	09/09/2021	Reviewed against AU and NZ legislation
1.3	30/06/2023	Formatting, Title and general policy Review
1.4	01/10/2026	Targeted update for current AU/NZ privacy requirements, credit reporting/Equifax process, cross-border disclosures, complaints, security and breach obligations