



SEPTEMBER 2026

Guide to Exercising Personal Data Protection Rights

Who Can Exercise Their Personal Data Protection Rights?

The exercise of data protection rights is strictly personal; that is, such rights may only be exercised by the data subject or by a legal or voluntary representative expressly designated by the data subject. If the request is made through a representative, proof of representation must be provided by any legally valid means.

How can you exercise your personal data protection rights?

Exercising these rights is free of charge and is initiated by submitting a request to the Acerinox Group company processing your personal data as Data Controller. However, provided that local regulations so permit, if requests are manifestly unfounded or excessive (e.g., repetitive in nature), the Group company acting as Data Controller may refuse to act or, where appropriate, charge a proportionate fee.

Since the Acerinox Group operates globally through various subsidiaries, each of which may act as the data controller for your personal data, you must specify in your request the Group company with which you wish to exercise your rights.

To exercise your rights, you may submit your request through the following channels, providing your identification and specifying the right you wish to exercise:

- Email: dpo@acerinox.com (for all Group companies except VDM Metals). Please include "personal data" in the subject line.
- Email: datenschutz.vdm@vdm-metals.com (exclusively for requests regarding data processed by VDM Metals).
- Mail: The request may be sent either to the address of the Group's Data Protection Officer ("DPO") (Calle Santiago de Compostela, 100, 28035 Madrid, Spain) or to the address of the Acerinox Group company's facility that processes the data subject's data. For VDM METALS, the request must be addressed to Plettenberger Straße 2, 58791 Werdohl, Germany. Any request received by mail will be forwarded without delay to the Group's Data Protection Officer, unless there is a local DPO designated to handle and respond to the request.

If we deem it necessary to identify you, we may request a copy of a document proving your identity.

Likewise, if the requester is acting on behalf of another person, they must provide proof of such representation through any means recognized by law.

What rights can you exercise as a data subject?

Data protection regulations recognize a series of rights for individuals whose data is being processed.

As the data subject, you may exercise the following rights:

- Right of access. You have the right to obtain confirmation as to whether your personal data is being processed and, if so, to access it.
- Right to rectification. Please note that by actively providing us with your personal data through any means, you guarantee that it is true and accurate and agree to notify us of any changes or modifications to it. You have the right to request the correction of your personal data when it is inaccurate or incomplete. In this case, you must specify which data is incorrect and provide, to the extent possible, documentation supporting the requested correction.
- Right to erasure. You have the right to request the erasure of your personal data when, among other circumstances, it is no longer necessary for the purpose for which it was collected, you withdraw your consent, you object to the processing, the data has been processed unlawfully, or it must be erased to

comply with a legal obligation. This right is not absolute and may be limited by legal retention obligations or other legitimate grounds.

- Right to restriction of processing. You have the right to request the restriction of the processing of your data in certain circumstances, such as when you contest the accuracy of the data (during the verification period), when the processing is unlawful but you do not wish to have the data erased, when the data is no longer necessary for the controller but you need it to assert legal claims, or when you have objected to the processing while it is being verified whether the controller's legitimate grounds override your interests.
- Right to data portability. You have the right to receive the personal data you have provided to a Group company in a structured, commonly used, and machine-readable format, as well as to request that such data be transmitted directly to another data controller when technically feasible. This right applies only when the processing is based on consent or a contract and is carried out by automated means.
- Right to Object. You have the right to object to the processing of your personal data when it is based on the legitimate interests of the data controller or on the performance of a task carried out in the public interest, including profiling. The data controller will cease processing the data unless it can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject. When the processing is for the purpose of direct marketing, you have the right to object at any time, without needing to provide a reason.
- Right to withdraw consent. Where the processing of your data is based on your consent, you have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. It shall be as easy to withdraw consent as to give it.
- Right to withdraw consent. Where the processing of your data is based on your consent, you have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. It shall be as easy to withdraw consent as to give it.

What are the response times and procedures?

Once your request is received, the Acerinox Group will send you an acknowledgment confirming receipt and inform you of the procedure that will be followed to respond to your request.

Generally, the maximum timeframe for responding to your request is one (1) month from the date of receipt. This timeframe may be extended by an additional two (2) months when necessary, considering the complexity of the request or the number of requests received. In the event of an extension, you will be notified of the reasons within the first month.

If the data controller determines that your request should not be granted, in whole or in part, it will provide you with a reasoned decision within one (1) month, informing you of your right to file a complaint with the competent supervisory authority and to pursue legal action.

The response will be provided via the same method you used to submit the request, unless you expressly specify a different method.

All requests received and responses issued will be duly recorded internally, in accordance with the proactive accountability obligations established in applicable regulations.

What options are available if you are not satisfied with the response you received?

If you believe that the processing of your personal data does not comply with current regulations, or if you are not satisfied with the response to your request to exercise your rights, you have the right to file a complaint with the competent data protection supervisory authority.

Below are the main supervisory authorities in the jurisdictions where the Acerinox Group has the strongest presence:

- Spain: Spanish Data Protection Agency (AEPD) — www.aepd.es

- Germany: Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the data protection authorities of each state (Bundesland).
- United Kingdom: Information Commissioner's Office (ICO) — ico.org.uk
- France: Commission Nationale de l'Informatique et des Libertés (CNIL) — www.cnil.fr
- Other EU countries: the competent national data protection authority of the relevant Member State.

For jurisdictions other than those indicated, please refer to Annex I of this Guide, which lists the competent supervisory authorities in each relevant country.

Adaptations by Jurisdiction

Due to the Acerinox Group's global presence, there are additional or specific requirements in certain jurisdictions that modify, supplement, or expand the rights and obligations described in the preceding sections.

These specific features are detailed in Annex I (Considerations by Jurisdiction) of this Guide, which includes specific information on applicable regulations, additional or different rights, specific timeframes, competent supervisory authorities, and the particular requirements of each jurisdiction.

This Guide has been drafted based on the general guidelines of the General Data Protection Regulation ("GDPR"). In the event of a conflict between its provisions and local regulations offering a higher level of protection to the data subject, the latter shall prevail.

ANNEX I — CONSIDERATIONS BY JURISDICTION

The following details the regulatory specifics of the main jurisdictions in which the Acerinox Group operates or has a significant presence. Each jurisdiction is presented in a separate section.

Country	Field	Detail
Argentina	Applicable legislation	Ley 25.326 de Protección de los Datos Personales (2000) and its Regulatory Decree 1558/2001.
	Specific rights	Access, rectification, update, erasure and confidentiality of personal data. Right to erasure (right to be forgotten) where data is inaccurate, incomplete, or its processing is prohibited. Habeas data action (Art. 33 et seq.).
	Timeframes	10 calendar days from receipt of the access request. 5 business days for rectification, update or erasure.
	Supervisory authority	Agencia de Acceso a la Información Pública (AAIP) — www.argentina.gob.ar/aaip .
Australia	Applicable legislation	Privacy Act 1988 and Australian Privacy Principles (APPs).
	Specific rights	Access and correction of personal data. No general right to erasure.
	Timeframes	30 days from receipt of the request.
	Supervisory authority	Office of the Australian Information Commissioner (OAIC).
Belgium	Applicable legislation	General Data Protection Regulation (GDPR) and Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions). Specific provisions on the processing of the national register number.
	Timeframes	1 month from receipt of the request, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Autorité de protection des données (APD) / Gegevensbeschermingsautoriteit (GBA) — www.autoriteprotectiondonnees.be .
Brazil	Applicable legislation	Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, in force since 18 September 2020.
	Specific rights	Confirmation of the existence of processing, access, correction of incomplete, inaccurate or outdated data, anonymisation, blocking or erasure of unnecessary, excessive or non-compliant data, portability, erasure of data processed on the basis of consent, information on public and private entities with which data has been shared, information on the possibility of denying consent and its consequences, withdrawal of consent, and right to request review of automated decisions.
	Timeframes	15 days from receipt of the request (pursuant to Art. 19 LGPD for confirmation and access requests). The ANPD may set differentiated timeframes by sector.
	Supervisory authority	Autoridade Nacional de Proteção de Dados (ANPD) — www.gov.br/anpd .
Chile	Applicable legislation	Ley 19.628 sobre Protección de la Vida Privada (legislative reform in progress).
	Specific rights	Access, rectification, cancellation and objection.
	Timeframes	Pending determination.
	Supervisory authority	Ordinary courts of justice (pending the establishment of the Data Protection Agency).
China	Applicable legislation	Personal Information Protection Law (PIPL), 2021.

Country	Field	Detail
	Specific rights	Access, copy, correction, erasure, portability and right to obtain an explanation of automated decisions.
	Timeframes	15 working days from receipt, extendable by 15 additional days.
	Supervisory authority	Cyberspace Administration of China (CAC).
Colombia	Applicable legislation	Ley 1581 de 2012 and Decreto 1377 de 2013.
	Specific rights	Access, update, rectification, erasure and withdrawal of consent.
	Timeframes	10 business days from receipt, extendable by 5 additional business days.
	Supervisory authority	Superintendencia de Industria y Comercio (SIC).
France	Applicable legislation	GDPR and Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés), as consolidated.
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions). Additionally, right to set directives regarding the retention, erasure and disclosure of personal data after the data subject's death (Art. 85 Loi Informatique et Libertés).
	Timeframes	1 month from receipt of the request, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Commission Nationale de l'Informatique et des Libertés (CNIL) — www.cnil.fr .
	Specific requirements	Specific legislation on health data (hébergement de données de santé). Mandatory DPO in the cases provided for by the GDPR.
Germany	Applicable legislation	Bundesdatenschutzgesetz (BDSG), supplementing the GDPR.
	Specific rights	Additional restrictions on the right of access (§34 BDSG). Obligation to notify third parties of rectifications. Erasure may be replaced by restriction of processing in certain circumstances.
	Timeframes	1 month (pursuant to the GDPR), extendable by 2 additional months.
	Supervisory authority	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) and the data protection authorities of each Land (Bundesland).
	Specific requirements	Mandatory DPO designation in expanded cases compared to the GDPR. VDM Metals has its own DPO: Contact: Adenauerallee 136, D-53113 Bonn Tel.: 0228/2272260 https://www.scheja-partner.de/kontakt/kontakt.html
Hong Kong	Applicable legislation	Personal Data (Privacy) Ordinance (PDPO), Cap. 486.
	Specific rights	Right of access to personal data (Data Access Request, DPP 6) and right of correction (Data Correction Request, DPP 6). No general right to erasure, portability or objection under the PDPO. Prohibition on the use of personal data for direct marketing without consent.
	Timeframes	40 days from receipt of the access request (Data Access Request).
	Supervisory authority	Office of the Privacy Commissioner for Personal Data (PCPD) — www.pcpd.org.hk .
	Specific requirements	The controller may charge a reasonable fee for handling access requests. 2021 amendments criminalizing doxxing (disclosure of personal data without consent with intent to cause harm). Obligation to adopt adequate security measures. No general international transfer regime in force (Section 33 PDPO not activated).
India	Applicable legislation	Digital Personal Data Protection Act (DPDPA), 2023.

Country	Field	Detail
	Specific rights	Access, correction, erasure and right to appoint a nominee.
	Timeframes	Pending determination by implementing regulations under development.
	Supervisory authority	Data Protection Board of India (in the process of being established).
Indonesia	Applicable legislation	Law No. 27 of 2022 on Personal Data Protection (UU PDP / Undang-Undang Pelindungan Data Pribadi).
	Specific rights	Access, rectification, update, erasure, withdrawal of consent, objection to automated decisions, restriction of processing, portability, and right to lodge a complaint. Right to compensation in case of a breach.
	Timeframes	For data subject rights requests, the timeframe must be "without undue delay."
	Supervisory authority	Personal data protection authority (in the process of being established). Until fully operational, the Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika / Kominfo) assumes supervisory functions.
Italy	Applicable legislation	GDPR and Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196), as amended by D.Lgs. 10 agosto 2018, n. 101.
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions). Specific rights regarding deceased persons, exercisable by those with a legitimate interest, acting for the protection of the data subject, or for family reasons deserving of protection.
	Timeframes	1 month from receipt of the request, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Garante per la protezione dei dati personali — www.garanteprivacy.it .
	Specific requirements	Specific sectoral legislation on data processing in the employment context (Art. 4 Statuto dei Lavoratori, Law 300/1970, regarding remote monitoring of employees). General authorization for special categories of data (provvedimenti del Garante).
Malaysia	Applicable legislation	Personal Data Protection Act (PDPA), 2010.
	Specific rights	Access and correction of personal data. No explicit general right to erasure.
	Timeframes	21 days for access requests.
	Supervisory authority	Jabatan Pelindungan Data Peribadi (JPDP) — Department of Personal Data Protection.
Mexico	Applicable legislation	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
	Specific rights	ARCO rights: Access, Rectification, Cancellation and Objection.
	Timeframes	20 business days from receipt of the request.
	Supervisory authority	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Peru	Applicable legislation	Ley 29733, Ley de Protección de Datos Personales.
	Specific rights	ARCO rights: Access, Rectification, Cancellation and Objection.
	Timeframes	8 business days for access; 10 business days for other rights.
	Supervisory authority	Autoridad Nacional de Protección de Datos Personales (ANPD).

Country	Field	Detail
Poland	Applicable legislation	GDPR and Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Personal Data Protection Act of 2018).
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions). Specific rules on video surveillance in the workplace (Art. 222 of the Labour Code).
	Timeframes	1 month from receipt, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Prezes Urzędu Ochrony Danych Osobowych (PUODO) — www.uodo.gov.pl .
	Specific requirements	Specific regulation on the processing of biometric data and video surveillance in the workplace. DPO certification in accordance with national criteria.
Portugal	Applicable legislation	GDPR and Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD na ordem jurídica portuguesa.
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions). Specific conditions for the processing of deceased persons' data.
	Timeframes	1 month from receipt, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Comissão Nacional de Proteção de Dados (CNPD) — www.cnpd.pt .
	Specific requirements	Additional restrictions on the processing of the civil identification number. Data subject consent required for certain processing of employee data.
Singapore	Applicable legislation	Personal Data Protection Act (PDPA), 2012.
	Specific rights	Access and correction of personal data.
	Timeframes	30 days from receipt of the request.
	Supervisory authority	Personal Data Protection Commission (PDPC).
	Specific requirements	Do Not Call Registry for direct marketing.
South Africa	Applicable legislation	Protection of Personal Information Act (POPIA), 2013.
	Specific rights	Access, correction and erasure of personal data.
	Timeframes	30 days from receipt of the request.
	Supervisory authority	Information Regulator.
South Korea	Applicable legislation	Personal Information Protection Act (PIPA/개인정보 보호법), as amended, and its implementing regulations.
	Specific rights	Access, correction, erasure, suspension of processing and withdrawal of consent. Right to request data portability (introduced by the 2023 amendment, with staggered entry into force). Enhanced rights regarding automated decisions (right to explanation and to request review by a natural person).
	Timeframes	10 days from receipt of the access request. 10 days for correction or erasure requests, during which processing of the data is suspended.
	Supervisory authority	Personal Information Protection Commission (PIPC/개인정보보호위원회) — www.pipc.go.kr .
	Specific requirements	Strict regime of separate consent for each purpose. Mandatory designation of a Chief Privacy Officer (CPO) for certain entities. Security breach notification to the PIPC and data subjects within 72 hours. Supplementary sectoral legislation (Credit Information Act for

Country	Field	Detail
		the financial sector). Specific regulation of pseudonymized data for statistical, research and archival purposes.
Sweden	Applicable legislation	GDPR and Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Dataskyddslagen).
	Specific rights	GDPR rights (access, rectification, erasure, restriction, portability, objection, automated decisions).
	Timeframes	1 month from receipt, extendable by 2 additional months (pursuant to the GDPR).
	Supervisory authority	Integritetsskyddsmyndigheten (IMY) — www.imy.se .
	Specific requirements	Supplementary sectoral regulation for data processing in the employment and healthcare contexts.
Switzerland	Applicable legislation	Revised Federal Act on Data Protection (nFADP / nDSG — Bundesgesetz über den Datenschutz), in force since 1 September 2023, and its Ordinance (DPO / DSV).
	Specific rights	Right of access (Art. 25 nFADP), rectification, erasure or objection to processing. Right to receive or have data transmitted in a commonly used electronic format (portability, Art. 28 nFADP). Right not to be subject to automated individual decisions (Art. 21 nFADP), with the right to be heard by a natural person.
	Timeframes	30 days from receipt of the access request. Where justified, the controller may postpone, restrict or refuse the disclosure.
	Supervisory authority	Federal Data Protection and Information Commissioner (FDPIC) / Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) — www.edoeb.admin.ch .
	Specific requirements	Switzerland is not a member of the EU/EEA. The European Commission has adopted an adequacy decision with respect to Switzerland. Obligation to maintain a record of processing activities. Obligation to carry out data protection impact assessments. Notification of data breaches to the FDPIC “as soon as possible.”
Taiwan	Applicable legislation	Personal Data Protection Act (PDPA/個人資料保護法), as amended.
	Specific rights	Access, request for copy, correction or supplementation of data, request for cessation of processing, use or disclosure, and erasure of personal data.
	Timeframes	15 days from receipt of the request, extendable by 15 additional days upon notice to the data subject.
	Supervisory authority	Ministry of Digital Affairs (MODA/數位發展部) as the main coordinating authority. Sector-specific supervision by the competent authorities of each industry (e.g., Financial Supervisory Commission for the financial sector).
	Specific requirements	Applicable to both the public and private sectors. Sanctions regime including civil and criminal liability. Restrictions on international transfers by resolution of the competent authority.
Thailand	Applicable legislation	Personal Data Protection Act (PDPA), B.E. 2562 (2019), fully in force since 1 June 2022.
	Specific rights	Access, portability, objection, rectification, erasure, restriction of processing, withdrawal of consent, and right to lodge a complaint with the competent authority.
	Timeframes	30 days from receipt of the request.
	Supervisory authority	Personal Data Protection Committee (PDPC) and Office of the Personal Data Protection Committee (OPDPC) — www.pdpc.or.th .
	Specific requirements	Explicit consent required for sensitive data. Mandatory security breach notification to the authority within 72 hours. Restrictions on international transfers unless the destination country has adequate protection standards.

Country	Field	Detail
Türkiye	Applicable legislation	Kişisel Verilerin Korunması Kanunu (KVKK), Law No. 6698.
	Specific rights	Rights similar to the GDPR: access, rectification, erasure and objection.
	Timeframes	30 days from receipt of the request.
	Supervisory authority	Kişisel Verileri Koruma Kurumu (KVKK).
United Arab Emirates	Applicable legislation	Federal Decree-Law No. 45/2021 on Personal Data Protection, together with the DIFC and ADGM regulations.
	Specific rights	Access, rectification, erasure, restriction, portability and objection.
	Timeframes	As per the applicable regulation (federal, DIFC or ADGM).
	Supervisory authority	UAE Data Office (federal), DIFC Commissioner of Data Protection and ADGM Commissioner of Data Protection.
United Kingdom	Applicable legislation	UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025 (Section 103, in force from 19 June 2026).
	Specific rights	Rights equivalent to the GDPR (access, rectification, erasure, restriction, portability, objection, automated decisions). New right of direct complaint to the controller (Section 164A DPA 2018, introduced by the Data (Use and Access) Act 2025).
	Timeframes	1 month from receipt, extendable by up to 3 months in complex cases.
	Supervisory authority	Information Commissioner's Office (ICO) — ico.org.uk.
	Specific requirements	EU adequacy decision in force. Mandatory complaint procedure from 19 June 2026 (*see subsection below).
	*Complaint procedure in the United Kingdom	
	The data subject may lodge a complaint regarding data protection matters with the Acerinox Group company that is the data controller through the following channels: • Email: dpo@acerinox.com • Post: addressed to the data controller or to the Group Data Protection Officer at calle Santiago de Compostela 100, 28035, Madrid, Spain. The complaint must include identification of the complainant and a description of the facts giving rise to the complaint, together with supporting documentation, where applicable. An acknowledgment of receipt of the complaint will be sent without undue delay. The maximum period for issuing a reasoned response is 1 month from receipt of the complaint. In cases of particular complexity, this period may be extended by 2 additional months, subject to prior reasoned communication to the complainant. The Group Data Protection Officer shall be responsible for managing the complaint. If the complainant is not satisfied with the response received, or has not received a response within the established period, they may lodge a complaint with the Information Commissioner's Office (ICO): • Web: ico.org.uk • Phone: +44 303 123 1113 Post: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom	
United States	Applicable legislation	No single federal data protection law. Key state laws: CCPA/CPRA (California), VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut).

Country	Field	Detail
	Specific rights	California (CCPA/CPRA): access, erasure, opt-out of data sales, limitation on the use of sensitive data, non-discrimination for exercising rights.
	Timeframes	45 days from receipt of the request, extendable by 45 additional days (California).
	Supervisory authority	California Privacy Protection Agency (CPPA) and California Attorney General. In other states, the State Attorney General.
	Specific requirements	Compliance with state laws based on the Group's presence and activity in each state.
Vietnam	Applicable legislation	Decree No. 13/2023/NĐ-CP on Personal Data Protection, in force since 1 July 2023.
	Specific rights	Access, rectification, erasure, restriction of processing, portability, objection to processing, withdrawal of consent, complaint, and right to compensation.
	Timeframes	For data subject rights requests, response without undue delay.
	Supervisory authority	Ministry of Public Security, through the Department of Cybersecurity and High-tech Crime Prevention (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao — A05).
	Specific requirements	Mandatory data protection impact assessments for sensitive or large-scale data processing. Explicit consent required for sensitive data. Local storage requirement and transfer of a copy of data to Vietnamese territory for certain controllers. Impact assessment dossier to be submitted to the Ministry of Public Security.