**The Dixon Group, Inc.**

**Privacy Notice for Employees - Overview**

Last updated: August 1, 2023

*This page provides a quick summary of the key information in this Privacy Notice. Please refer to the full notice below for further details.*

|  |  |
| --- | --- |
| **Employer**  **(Controller)** | The Dixon Group, Inc. (and its related affiliated companies)  **Email:** [dixonhr@dixonvalve.com](mailto:dixonhr@dixonvalve.com)  **Phone:** 1-833-976-1849 (Privacy #)  **Post:** Dixon Group HR, 1 Dixon Square, Chestertown, Maryland 21620 |

|  |  |
| --- | --- |
| **Information we hold about you**  A summary of the types of information we collect about you | |
| Information we collect:   * Identity & contact details * Recruitment info * Pay and benefits * Employment/performance records * Correspondence * Use of IT and other systems | Sensitive Information:   * Medical records / health data * Racial or ethnic origin * Criminal records * Trade Union membership * Legally protected characteristics (e.g., under US state laws) |

|  |  |
| --- | --- |
| **Reasons we use your information**  The main reasons we collect and use your information | |
| * Recruitment and appointment * Managing your employment and benefits * Managing our business * Managing HR and our employees * Background checks and screening | * Legal claims * Detecting or preventing fraud or other crimes * Complying with our legal obligations * Protecting someone’s vital interests |

|  |  |
| --- | --- |
| **Disclosing your information** | **Your Rights** |
| We may disclose your information with third parties for the purposes of:   * Providing and managing IT systems * Managing security measures * Staff development and training * Addressing Legal Claims * Managing employee benefits * Background checks and screening * Complying with our legal obligations | Depending on your location, you may have the following rights:   * Right of Access * Right to Rectification * Right to be Forgotten * Right to Object * Right to Restriction of Processing * Data Portability * Withdrawal of Consent * Complaints * Protection against discrimination/retaliation |

**The Dixon Group, Inc.**

**Privacy Notice for Employees**

Last updated: August 1, 2023

**1. About this notice**

This is a notice for all employees, job applicants and other workers of the Dixon Group (meaning The Dixon Group, Inc. and its related affiliated companies).

As your employer, we collect and hold personal information about you in relation to your employment with us. This notice explains how and why we collect, use, and disclose your personal information, as well as the rights that you have in respect of your personal information.

If you have any questions about your privacy at work, or how we use your personal information, please email us at [dixonhr@dixonvalve.com](mailto:dixonhr@dixonvalve.com) or call us on **1-833-976-1849** (Privacy #).

For the Dixon Group’s general privacy policy, please refer to the following link: https://dixonvalve.com/en/privacy.

**2. How we collect your information**

Most of the information that we hold about you is either collected directly from you (during the recruitment process or your employment with us) or generated by us in the course of your employment.

We may also obtain information about you from other sources, for example:

* During the recruitment process, we may obtain references from your previous employers as well as information from recruiters and job-search and social media platforms.
* We may obtain information about you from third parties for checks or screening purposes, such as the results of background checks, drug tests, or physical/medical screening tests where these are required for particular roles.
* We may receive information from third parties involved in the investigation or administration of workplace claims.

There are circumstances where we require you to provide us with data in order to proceed with the employment relationship. If you fail to provide that information, we may be prevented from performing our obligations to you (such as paying you or providing benefits) or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees).

**3. The types of information we hold**

We explain below the different types of personal information that we may hold about you, depending on your role with us.

* **Identity and contact details** – such as your full name, title, gender, date of birth, employee ID number, marital status, beneficiaries, dependents, next of kin or other emergency contacts, photographs and physical descriptions, addresses, phone numbers, and email addresses
* **Your legal identity and right to work** – such as copies of your passport, driving licence, state ID card or other identification documents, any evidence in relation to your right to work in the US and your social security number.
* **Recruitment information** – such as references, education and employment history, skills and qualifications and other information included in your CV or resume.
* **Pay and benefits** – details of your salary or wages and any deductions, expenses and reimbursements, your bank details and other financial information for payments, your tax status and details of benefits including pension or retirement plans and insurance.
* **Employment and performance records** – such as information about your work, your employment contract with us, your attendance, leave and absences, performance, training and development, your start and end dates and your reason for leaving, any disciplinary or grievance procedures and other information related to your role with us.
* **Correspondence and your use of our systems** – such as emails, letters, recorded phone calls and other correspondence, passwords and other login credentials, details of your activity on work computers or other devices, the internet or on Dixon Group IT systems including records of access to files, databases or other systems or physical locations, and metadata from work devices which may include geolocation data.

We may also hold the following types of more sensitive information about you:

* **Medical or health-related data** – we may hold information about your health or medical records, for example in relation to sick leave, health insurance plans, disabilities, accidents at work or pre-work screening checks (including drug tests).
* **Racial or ethnic origin** - we may hold information about your racial, ethnic or national origin for equal employment opportunity monitoring purposes.
* **Criminal record** – we may obtain information about criminal convictions or offences, for example, where background checks are required for a particular role.
* **Trade Union membership** – we may hold information about your membership or association with trade unions or similar industry bodies.
* **Other protected characteristics** – we may hold information about other characteristics that are protected under state or federal law, including information about your age, sex, gender or gender identity, marital status, citizenship, primary language, immigration status or military/veteran status.

**4. How and why we use your personal information**

We only collect personal information about you where we have a specific and legitimate purpose to do so in connection with your employment with us. In this section, we explain the purposes for which we use your information.

***Legal basis for processing personal information***

*The General Data Protection Regulation (GDPR) in the UK and EU sets a high standard for the protection of personal data compared to the US and other nations. Dixon Group is a global organisation and aims to achieve this level of data protection across the group.*

*The GDPR requires that businesses have a specific legal basis to use individuals’ personal information. As well as explaining the purposes for which we use your personal information, in this section we explain our legal basis for that use of your information.*

**Recruitment and appointment**

We need to use your personal information during the recruitment process and your appointment to a position with us. For example, we use your information in order to:

* Assess your skills, qualifications and experience
* Make decisions about your recruitment or appointment
* Determine the terms on which you will work for us
* Check you are legally entitled to work at your location of employment
* Determine your tax status

The information we use in this context includes the “Recruitment information” set out in section 3 above and may include information received from third parties such as recruiters, past employers, job-search platforms, social media platforms and background or credit check agencies.

Our legal basis for using your information in this context is that it is necessary in order for us to take steps, at your request, towards entering into an employment contract with you.

**Your employment contract and benefits**

Even if it is not in writing, there is a legally binding employment contract between you and us –you agree to work for us and follow our rules and policies, and we agree to pay you, provide certain benefits and otherwise manage your employment.

We need to use your personal information in order to perform our side of that contract, for example in order to:

* Pay you and make any relevant deductions
* Provide benefits to you, including training and development, insurance policies and retirement or pension benefits
* Enrol you in, and manage, retirement or pension arrangements including 401(k) arrangements
* Administer the contract between us

We may need any of the information that we hold about you for these purposes, and our legal basis for using your information in this way is that it is necessary in order for us to perform our obligations under the contract between us.

**Managing our business**

We use your personal information for various business purposes relating to the management of the organisation. For example, we may use your information in order to:

* Undertake business management and planning, including accounting and auditing
* Provide and manage education, training and development for employees
* Monitor the use of our information and communication systems to ensure compliance with our IT policies
* Comply with health and safety and other legal regulations
* Ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems
* Undertake equal employment opportunities monitoring

We may need any of the information that we hold about you for these purposes. Where this forms a part of our obligations under the employment contract, our legal basis for using your information in this way is that it is necessary for the performance of that contract.

In some cases, we may be required to use your information for these purposes in order to comply with our legal obligations (for example, in respect of complying with health and safety laws).

We may also use your information for these purposes to pursue our legitimate interest in effectively managing our business, where we consider it fair and reasonable to do so, taking into account your rights to privacy.

**Managing our employees**

As an employer, we need to use information about our employees in order to effectively manage our workforce, such as in order to:

* Conduct performance reviews, manage employee performance and determine performance targets or requirements
* Make decisions about salary reviews and compensation
* Assess qualifications or skills for a particular job or task, including decisions about promotions
* Gather evidence for possible grievance or disciplinary procedures
* Make decisions about your continued employment or engagement
* Make arrangements for the termination of our working relationship
* Deal with any legal disputes involving you or other employees, including in relation to accidents at work
* Ascertain your fitness to work or to perform a particular role or task
* Manage sickness and other absences

Where this forms a part of our obligations under the employment contract, our legal basis for using your information in this way is that it is necessary for the performance of that contract.

We may also use your information for these purposes to pursue our legitimate interest in effectively managing our employee base, where we consider it fair and reasonable to do so, taking into account your rights to privacy.

**Other purposes**

In limited circumstances, there may be other purposes for which we use your personal information. This may include, for example:

* To detect and prevent fraud or other illegal activity
* To comply with any legal obligations
* To protect the vital interests of you or another individual (for example, in the case of an emergency or injury)

Some of the grounds for using your personal information set out in this notice may overlap, and we may have multiple reasons and legal bases to justify the use of your information. Please note that we may process your personal information without your knowledge or consent where this is required or permitted by law.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

**How we use sensitive personal information**

Some of the information we hold about you may be particularly sensitive or otherwise represent data or characteristics that are protected by law.

**Health data**

We may use information about your health or healthcare for the following purposes:

* Managing sick leave
* Making reasonable accommodations for any medical conditions or disabilities
* Carrying out drug screening tests and drug testing, as part of the recruitment process or during your employment in order to ensure and monitor health and safety at work
* Obtaining medical certificates required for commercial licence drivers and disclosing these to relevant third parties where necessary
* Handling legal claims such as workplace compensation claims
* Managing and providing employee health insurance

**Racial or ethnic origin**

We may hold information about your racial, ethnic or national origin. We collect and use this data only for the purpose of monitoring equal employment opportunities.

**Criminal convictions and offences**

We may collect information relating to any criminal convictions or offences where we undertake background or criminal record checks prior to or during the term of your employment.

We may use information from background checks to determine your suitability or eligibility for a certain role and, if your role involves any driving for the company, we may carry out checks of your driving licence record as part of our efforts to ensure the health and safety of our employees.

**Trade Union Membership**

We may hold information about your membership of a trade union or association. We use this information only for the purposes of managing any specific benefits or restrictions for union employees and for calculating your wages and any relevant deductions (such as union dues).

**5. Limited sharing of personal information**

We may share your personal information with third parties where required by law, where it is necessary in connection with your employment with us or where we otherwise have a legitimate business interest to do so.

**Service Providers which access your data on our behalf**

We use various third-party services to help manage our business and HR processes and it is necessary for us to share your information with those organisations.

We retain full control of your information and we put in place safeguards, including contractual restrictions, to ensure that your information is used only in accordance with our instructions. We may share your data in this context with third parties for the purposes of:

* Providing and managing our IT systems, including managing our HR systems and software, cloud computing and storage, website hosting and managing staff user accounts.
* Managing physical and technical security systems, such as identity management (single sign-on, multi-factor authentication etc.) and access restrictions at our physical premises
* Staff development and training, including our learning management systems.

**Other third parties we share your information with**

We may also need to share information about you with third parties in other contexts, for example:

* **Legal Claims** – we may need to share information about you, including information about your health, with our professional advisors in connection with any legal claims involving you, including worker’s compensation claims.
* **Managing benefits** – we may share your information with third parties for the purpose of providing and managing certain benefits, such as 401(k) and other retirement plans and insurance policies including health insurance (which may include information about your health).
* **Background checks** – we may share information about you with third party providers of screening services for the purpose of carrying out background checks or drug or other health screening tests.
* **Our legal obligations** – we may share information about you with third parties, such as Government departments, for the purposes of managing our legal obligations including tax and compliance obligations.

We may also share information about you with third parties in exceptional circumstances, such as in case of emergency (for example to protect the vital interests of you or another person), to fulfil our legal obligations, for public interest reasons (for example to prevent or detect fraud or other illegal activity), or in the context of a sale or restructuring of part of our business.

**Cross-border sharing of your information**

The Dixon Group is a global business and it may be necessary for us to share your data with other Dixon locations or with third parties located in other countries.

We always ensure that safeguards (such as contractual or legal obligations) are in place to keep your information secure and that we comply with all applicable data protection laws relating to international transfers of personal data. For example, where the UK or EU GDPR apply to our use of your information, we use standard contractual clauses issued by the UK and EU authorities to provide appropriate safeguards for these transfers.

**6. How long we keep your personal information**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

We will retain most of the information that we hold about you throughout the duration of your employment with us (unless it is no longer necessary for us to hold it) and for a certain period after your employment in accordance with legal or industry guidelines. For example, we may retain information about you after the end of your employment for tax, accounting or compliance purposes, or to manage potential legal claims.

Detailed information about how long we retain specific types of information about you is set out in our Data Retention Policies, which are available from our HR department ([dixonhr@dixonvalve.com](mailto:dixonhr@dixonvalve.com)).

**7. Your Rights (UK and EU employees)**

If you are based in the UK or EU, you have a number of rights available to you in respect of your personal information, which are explained below.

Some of these rights only apply in certain circumstances, and these legal rights may not be available to employees in other locations (including in most US states). If you wish to exercise any of these rights or have questions about the rights available to you, please contact the HR department using the details at the top of this notice.

**Access**

The right of access allows you to obtain information about how we collect and use your personal data (including information about any disclosure, sharing or sale of your data), as well as copies of the information that we hold.

**Rectification**

The right of rectification allows you to request that we update or correct information that we hold about you, if it is incorrect or outdated.

**Erasure (the right to be forgotten)**

The right of erasure (also known as the “right to be forgotten”) allows you to request that we delete some or all of the information that we hold about you. This right is only available in certain circumstances, including where:

* we no longer need the data for the purpose it was collected for;
* we rely on your consent, and you withdraw that consent;
* you object to our use of your data (see “Objections” below) and there are no overriding reasons for us to continue holding that data;
* we have used your data unlawfully; or
* there is a legal requirement to erase your data.

If you request erasure of your information in circumstances other than those above, we may not be able to comply with your request (for legal or administrative reasons).

**Objections**

You have the right to object to our use of your information:

* where we rely on our legitimate interests as our legal basis; or
* where we use your information for direct marketing purposes.

Please see section 4 (“*How and why we use your personal information*”) above for more information about the circumstances where we rely on a legitimate interest as our legal basis for using your information. We do not carry out direct marketing to our employees.

If you object to our use of your information, we will stop that use unless there is a compelling, legitimate reason for us to continue.

**Restriction of Processing**

You have the right to request that we stop using your information (but still retain it) in the following circumstances:

* you tell us that the information is inaccurate (until we can verify its accuracy);
* we have used your information unlawfully (but you do not wish us to delete it);
* we no longer need the information for the purpose it was collected for, but we still need it in connection with a legal claim; or
* you have objected to our use of the data (see “Objections” above), while we review your objection.

**Data Portability**

You have the right to request that we transfer your information (in a commonly used electronic format) to another organisation.

**Withdrawal of Consent**

In any circumstances where we rely on your consent to use your information, you have the right to withdraw that consent at any time and for any reason. If you do, we will stop using your information in that context.

**Automated Decision Making**

You have the right not to be subject to decisions made solely by automated means (e.g., by a software algorithm) which may produce significant effects for you – such as decisions which affect your employment or your legal rights.

We do not use automated decision-making to make any significant decisions about you. If you have any concerns or questions about this, you may contact our HR department.

**Complaints**

Depending on where you are based, you may have the right to lodge a complaint with the national data protection supervisory authority. For example, in the UK, complaints may be submitted to the Information Commissioner’s Office ([www.ico.org.uk/make-a-complaint](http://www.ico.org.uk/make-a-complaint)).

This process may not be available to you if you are based in the US or other locations. However, if you wish to make a complaint about our use of your information, please contact our HR department ([dixonhr@dixonvalve.com](mailto:dixonhr@dixonvalve.com)) and we will handle it through our internal complaint procedures.

**8. Specific information for California residents**

California state law requires us to provide information in a certain format to Californian employees about our collection and use of your data for the purposes of the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

This section sets out additional information we are required to provide under the CCPA and CPRA.

**Your Rights**

You have the following rights in respect of your personal data. Dixon Group complies with all such obligations to the fullest extent required by applicable law. Please note that these rights are only legally available to California residents.

|  |  |
| --- | --- |
| **Right to Know** | **Right of No Retaliation** |
| You have the right to request information about:   * The categories of personal data collected about you. * Specific pieces of personal information collected about you. * The categories of sources from which we collect personal information. * The purposes for which we use your personal information. * The categories of personal data that we sell or share with third parties, and the corresponding categories of third-party recipients. * The categories of personal data that we disclose to third parties for specific business purposes, and the corresponding categories of third-party recipients. | You have the right not to be discriminated against or otherwise subjected to any retaliation as a result of you exercising any of your rights under data protection and privacy laws.  This means that we will not treat you any differently because you have exercised these rights. |
| **Right to Request Deletion** | **Right to Correct** |
| You have the right to request deletion of the personal information that we have collected about you, subject to certain exemptions (such as where the information is used by us to detect security incidents or to comply with a legal obligation). | You have the right to request correction of any inaccurate personal information that we maintain. |
| **Right to Limit Use and Disclosure** | **Right to Opt Out** |
| You have the right to limit the use and disclosure of your sensitive personal information, and therefore you can direct us to limit the use of such sensitive personal information for permitted business purposes. | We do not sell or share personal information for purposes to which the right to opt out of sale or sharing applies under the CCPA. |

**Where We Get Your Information**

We collect information about you from the following sources:

* You
* Prior employers, references, recruiters, job-related social media platforms
* Third-party sources of demographic information
* Third-party companies, such as background check companies, drug testing facilities
* Claim administrators and investigators.

Depending on the Company’s individual interactions with you, we may or may not collect information about you from all of these categories of sources.

**Categories of Personal Data collected**

We may collect the following specified categories of personal information:

|  |
| --- |
| Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers. |
| Personal data as described in §1798.80(e) - any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. |
| Characteristics of protected classifications under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language, immigration status, military/veteran status, disability, request for leave, and medical conditions. |
| Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. |
| Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website application, or advertisement. |
| Geolocation data |
| Audio, electronic, visual, thermal, olfactory, or similar information |
| Professional or employment-related information |
| Non-public education information |
|  |

The CPRA defines the following as sensitive personal information:

|  |
| --- |
| Personal data that reveals your social security, driver’s license, state identification card, or passport number |
| Personal data that reveals your account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account |
| Personal data that reveals your precise geolocation |
| Personal data that reveals your racial or ethnic origin, religious or philosophical beliefs, or union membership |
| Personal data that reveals the contents of your mail, email, and text messages (except where we are the intended recipient of the communication) |
| Information about your health |
| Information about your sex life or sexual orientation |

**How Your Personal and Sensitive Personal Information is Used.** We may collect personal information about you for the following *specified business purposes*, as defined in the CPRA:

1. To comply with state and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records);
2. To process payroll;
3. To maintain commercial insurance policies and coverages, including for workers’ compensation and other liability insurance;
4. To manage workers’ compensation claims;
5. To administer and maintain group health insurance benefits, 401K and/or retirement plans;
6. To manage employee performance of their job duties;
7. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct);
8. To evaluate job applicants and candidates for employment or promotions;
9. To obtain and verify background checks on job applicants and employees;
10. To evaluate, make, and communicate decisions regarding an employee’s employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline.
11. To grant employees access to secure Company facilities and maintain information on who accessed the facility; and
12. To implement, monitor, and manage electronic security measures on employee devices that are used to access Company networks and systems;
13. To evaluate and/or defend against legal claims. (Dixon Group reserves all rights with respect to the attorney-client privilege and attorney-work product.)

By way of example, the following chart illustrates how certain categories of personal information are used for the above business purposes, as referenced generally by number. This chart is not an exhaustive or binding list, and Dixon Group may collect, use, or disclose any of the above personal information for business purposes to the extent otherwise allowed by law.

|  |  |  |
| --- | --- | --- |
| **CATEGORY** | **EXAMPLES** | **BUSINESS PURPOSE** |
| Personal Identifiers | Name, alias, employee ID number, postal or mailing address, email address, telephone number, social security number, driver’s license or state identification card number, passport number | 2, 3, 4, 6, 7, 8, 9, 13 |
| Physical Characteristics | Eye color, hair color, hair style, height, weight, build, tattoos, piercings | 11, 13 |
| Financial Information | Bank account number, credit card number, debit card number, or other financial account information | 2, 13 |
| Protected Classifications | Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religion, age, disability, medical or mental condition, military status, familial status, language | 1, 5, 7, 13 |
| Pre-Hire Information | Job application, resume, background check results, drug test results, job interview notes, and candidate evaluation records | 7, 8, 9, 10, 13 |
| Professional or Employment-Related Information | Personnel file, new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury and safety records, performance evaluations, disciplinary records, training records, licensing and certification records, compensation and health benefits records, and payroll information and records | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13 |
| Medical and Health Information | Doctor’s notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, and correspondence with employee and his/her medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as post-hire drug test results | 1, 4, 5, 7, 13 |
| Education Information | Transcripts or records of degrees and vocational certifications obtained | 6, 8, 10, 13 |
| Visual, Audio or Video Recordings in the Workplace | Surveillance cameras or pictures of employees taken in the workplace or at a Company function or event | 6, 13 |
| Facility Access Records | Information identifying which employees accessed secure Company facilities and at what times using their keys, badges, fobs or other security access method | 11, 13 |
| Geolocation Data | IP address and/or GPS location (latitude & longitude) recorded on Company-issued computers, electronic devices, and vehicles, as well as timekeeping applications on cell phones that employees use to clock in and out and that log the geographic location at which each time entry was made | 6, 12, 13 |
| Internet and Network Activity | Internet or other electronic network activity information on Company-issued computers and electronic devices, including browsing history, search history, and usage history | 12, 13 |
| Mobile Device Security Information | Data identifying employee devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider | 12, 13 |

**Inferring Characteristics from Sensitive Personal Information**

For purposes of the CCPA and CPRA, Dixon Group **does not** infer characteristics from sensitive personal information, nor has it done so at any time subsequent to December 31, 2022.

**Selling and Sharing Personal Data**

Under the CPRA:

* “Selling” personal information means a transaction whereby personal data is exchanged for monetary or other valuable consideration.
* “Sharing” personal information means disclosing or otherwise making personal information available to a third party for the purposes of for cross-context behavioural advertising.

We do not (nor have we done at any time since January 1, 2022) sell or share your personal information. We do not (nor have we done at any time since January 1, 2022) knowingly sell or share the Personal Information of minors under 16 years of age.

**Protecting Your Personal Information**

The above Personal Information may be disclosed as needed to various Dixon Group Officers, Directors, Human Resources personnel, accounting personnel, legal representatives, insurers and, in some instances, limited supervisory employees with a bona fide need to know. Not all categories of Personal Information are shared with all Dixon Group personnel, but only as necessary to carry out business purposes recognized by applicable law. All Dixon Group employees who are reasonably anticipated to have access to any form(s) of personal information receive training about their obligations to maintain the confidentiality of such sensitive information.

**Data Retention**

Dixon Group generally retains the information it receives about you for a period of six (6) years, unless a shorter or longer period is required by applicable California or federal law.

**For Inquiries and/or to Submit Requests for Information, Deletion or Correction.** To the fullest extent required by law, Dixon Group allows applicants and employees to inquire about and delete or correct certain categories of personal information.

Please contact Dixon Group Human Resources, 800 High Street Chestertown, Maryland 21620, 410-778-2000 or email [dixonhr@dixonvalve.com](mailto:dixonhr@dixonvalve.com) or call 1-800-xxx-xxxx to discuss any inquiries or concerns about the Company’s privacy policy and/or to submit your requests for information, deletion or correction. All requests for information, deletion, or correction of personal information must include sufficient detail that allows the Company to properly understand, evaluate, and respond to it.

The Dixon Group may not be able to comply with certain requests to know, such as in the following circumstances:

* We do not maintain the personal information in a searchable or reasonably accessible format
* We maintain the personal information solely for legal or compliance purposes
* We do not sell the personal information or use it for any commercial purpose

Additionally, the Dixon Group may be prohibited by law from producing certain highly sensitive personal information in response to a request for specific pieces of personal information. This may include Social Security numbers, login credentials, and health insurance numbers.

Any response will explain the reasons the Company cannot comply with the request, if applicable.

**Verification**

Upon receipt of such requests, the Dixon Group will take reasonable steps to confirm that the individual submitting the request is the individual to whom the information relates (or his or her authorized agent), and to prevent unauthorized access to, correction of, or deletion of information. In order to verify such requests, the Company will match identifying information provided by the individual to the personal information of the individual already maintained by the Company.

**Authorized Agents**

You can designate an authorized agent to make a request on your behalf by one of the following:

1. Explicit Written Consent
2. Power of Attorney
3. A parent or guardian may also make a verifiable consumer request on behalf of his or her minor child.

We may deny a request from an authorized agent if the agent does not submit proof that the consumer has authorized them to act on his or her behalf.

**Timing**

The Dixon Group will confirm receipt of a request to know, correct, or delete within 10 business days of receiving the request. We will attempt to respond to a verified request to know, correct, or delete within 45 days of its receipt, but we may require more time, in which case we will inform you of the reason for the delay.

Any disclosures provided will only cover the 12-month period preceding the verifiable request’s receipt.

**No Retaliation**. Dixon Group is committed to full compliance with the California Privacy Rights Act (“CPRA”) and any and all other laws pertaining to employee privacy rights. To that end, employee and/or applicant inquiries about their privacy rights are always welcome, and no employee or applicant will experience discrimination and/or retaliation of any kind for inquiring about and/or asserting their privacy rights.

**9. Changes to this Notice**

If we intend to use your information in ways that are not explained in this notice, we will either contact you first to explain this (in ad-hoc cases) or we will update this notice to explain the new use of your information.

This notice will be reviewed on at least an annual basis. We will notify you when we make significant changes to this notice, but we may also make minor changes to this notice without notifying you. If you have questions about how we use your information or if you wish to see the most up-to-date information, we recommend that you check the latest version of this notice.

This notice was last updated on the date stated at the top.