



Crawford & Company Corporate Policy

Global Data Protection and Privacy

1. Objectives

It is the policy of Crawford & Company and all of its Affiliates (“Crawford”) to comply with all applicable data protection and privacy laws. This document defines the fundamental business rules that enable Crawford as an organization to comply with the requirements associated with these laws and reflects the importance Crawford places on earning and keeping the trust of our employees, clients, claimants, and others who share personally identifiable information (“PII”) with us. Generally, Crawford makes reasonable efforts to protect PII from unauthorized use or disclosure. To this end, Crawford will ensure that it collects, uses, retains, discloses, and disposes of PII in conformity with the privacy principles set forth in the Generally Accepted Privacy Principles (“GAPP”), which reflect internationally recognized fair information practices included in data protection and privacy laws and regulations of various jurisdictions around the world.

2. Background

- 2.1 Data Privacy is generally defined as the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and disposal of PII. PII is information recorded in any form or format that can be used to specifically identify an individual data subject.
- 2.2 Maintaining the privacy of PII is a key part of corporate governance and accountability. It is a key business imperative as Crawford business systems and processes become increasingly complex and sophisticated. In the wake of this complexity and sophistication, Crawford is collecting increasing amounts of PII that is increasingly vulnerable to a variety of risks, including loss, misuse, unauthorized access, and unauthorized disclosure.
- 2.3 These increasing vulnerabilities raise concerns for Crawford, for its clients, and for data subjects. Like many organizations, Crawford seeks to strike a balance between protection of PII and the collection, use, and disclosure of PII that facilitates business processes. At the same time, data subjects are very concerned about their PII, and are particularly concerned about identity theft that may result from inappropriate or unauthorized access to PII, particularly financial or medical information. In short, failure to enact and follow adequate privacy policies and procedures may cause damage to Crawford's reputation, brand, or business relationships, may create legal liability and regulatory sanctions, and may result in employee, client, or claimant distrust. These consequences may ultimately result in lost business, including revenue and market share loss.
- 2.4 To help it comply with a wide variety of international, national, and local laws and regulations, Crawford will base its privacy policies and procedures on GAPP privacy principles that are founded on key concepts from significant international, national, and local laws, regulations, guidelines, as well as good business practices followed by organizations around the world. This allows Crawford to proactively address the significant challenges it faces in establishing and maintaining its privacy program to manage multi-jurisdictional privacy risks.
- 2.5 The following is a list of the Data Protection and Privacy principles to which Crawford will adhere:

2.5.1. Limitations on Collection, Use, Retention, Disclosure, and Disposal of PII

- 2.5.1.1. **Notice and Consent** – Crawford will collect and process PII fairly and lawfully and, where appropriate, with the knowledge or consent of the data subject. Where appropriate, Crawford will provide notice about its privacy policies and procedures, identify the purpose for which PII is collected, used, retained, and disclosed, and obtain implicit or explicit consent with respect to the collection, use, and disclosure of PII. The type of notice or consent required will depend on the context and circumstances, the sensitivity of the PII, the data subject's reasonable expectations, and legal requirements.
- 2.5.1.2. **Collection Purpose and Proportionality** – Crawford will collect PII only for specific, limited, and legitimate purposes. The PII collected will be relevant, adequate, and not excessive for the purposes for which it is collected or to which the data subject subsequently consents.
- 2.5.1.3. **Limitations on Use, Retention, and Disposal** – Crawford will not process PII in a manner inconsistent with the purposes for which it was originally collected without first obtaining the data subject's consent and, where appropriate, Crawford will limit the use of PII to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Crawford will not use PII for direct marketing purposes without the data subject's express or implied consent, depending on the circumstances and legal requirements. Crawford will not make decisions based solely on automated processing of PII except as permitted by applicable law. Crawford will not retain PII in a form that permits identification of data subjects for longer than

necessary to fulfil the stated purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory requirements or to fulfil client requests. Crawford will appropriately dispose of the information when it is no longer needed to fulfil the stated purposes for which it was collected or to which the data subject has consented.

2.5.1.4. **Disclosure** – Crawford will disclose PII to third parties only for the purposes identified in the notice and, where required, with the implicit or explicit consent of the individual, unless legal requirements compel disclosure regardless of whether Crawford has obtained consent. Crawford will take appropriate measures, by contract or otherwise, to provide adequate protection for PII that is disclosed to a third party.

2.5.1.5. **Cross-Border Data Transfers** – Crawford will take appropriate measures, by contract, consent or otherwise, to provide adequate protection for PII that is transferred from one country to another, including transfers among affiliates. If consent is the method used to provide adequate protection, the type of consent obtained (implicit or explicit), will depend on the context and the circumstances, the sensitivity of the PII, the data subject's reasonable expectations, and legal requirements.

2.5.2. Management of PII

2.5.2.1. **Management** – Crawford will define, document, communicate and assign accountability for privacy policies and procedures, including the designation of personnel within Crawford who are accountable for compliance with privacy and data protection laws and associated policies and procedures.

2.5.2.2. **Quality** – Crawford will take appropriate steps to ensure that PII it maintains is accurate and reliable for its intended use and, where necessary for its intended use, kept up-to-date.

2.5.2.3. **Access** – Crawford will maintain procedures to provide data subjects with appropriate access to their PII for review and, when appropriate, an effective means to have their PII corrected or deleted.

2.5.2.4. **Security of PII** – Crawford will implement reasonable administrative, physical, and technical security measures to protect PII from unauthorized access, unauthorized use, and unauthorized or accidental destruction, modification, or disclosure. Crawford will provide a level of security appropriate to the risks and the sensitivity of the PII.

2.5.3. Accountability and Enforcement

2.5.3.1. **Monitoring and Enforcement** – Crawford will monitor compliance with its privacy policies and procedures using internal controls for verifying compliance with privacy and data protection laws and with Crawford privacy policies and procedures.

2.5.3.2. **Complaint Process** - Crawford will provide a fair process for investigating and resolving privacy-related complaints and objections and will take appropriate steps to communicate that process to data subjects.

3. Scope

- 3.1 This policy applies to all Crawford employees (including contract employees) and covers all PII processed by Crawford, whether it relates to internal or external data subjects, and no matter where it is processed.

4. Definitions

- 4.1 “Data Subject” generally means a natural person who can be individually identified, directly or indirectly, in particular by reference to an identification number, including a social security number, or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity. Note, however, that in certain countries, e.g. Switzerland and Italy, the term “data subject” may also refer to legal entities.
- 4.2 “Personally Identifiable Information (PII)” means any information recorded in any form or format relating to an identified or identifiable data subject.
- 4.3 “Process” or “Processing” means doing anything with PII, whether or not by automatic means, such as collecting, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, accessing or providing access to, combining, erasing, or destroying PII.
- 4.4 “Affiliate” means any entity that is controlled, directly or indirectly, by Crawford.

5. Approach

- 5.1 The Crawford Privacy Office will review each GAPP principle and determine whether creation of a detailed global procedure to implement the principle is required and/or feasible.
- 5.2 Responsibility
- 5.2.1. Americas Privacy Director - Drafts and maintains the Americas provisions in privacy Procedures and responds to questions about Crawford’s privacy practices in the Americas; Provides input to Internal Audit regarding periodic auditing and monitoring activities.
- 5.2.2. EMEA/AP Privacy Manager - Drafts and maintains the EMEA/AP provisions in privacy Procedures and responds to questions about Crawford’s privacy practices in the EMEA/AP; Provides input to Internal Audit regarding periodic auditing and monitoring activities.
- 5.2.3. Internal Audit - Implements periodic auditing and monitoring activities to assess compliance with privacy and data protection policies and procedures
- 5.2.4. Operations Personnel – Those employees and contractors who interact with data subjects will understand and abide by this Policy.
- 5.3 Compliance
- 5.3.1. Compliance with this Policy and its associated procedures is mandatory for all Crawford employees and contractors.

Ownership and Control

Document Detail	
Unique Reference No. (URN)	DPPOL001 – Global Data Protection and Privacy Policy
Category	Policy
Version	0.1
Original Issue Date	April 30, 2012
Latest Review Date	March 12, 2018
Expiry Date	None

Intellectual Property

This document is marked “© Crawford & Company”. Crawford and Company asserts its intellectual property rights in relation to this document.

This document cannot be fully or partially copied or replicated, or altered in any way, or disclosed outside Crawford without the express permission of the Sponsor or Author. Where an individual, organisation or business is in possession of this document, they may not cause or allow the document or any of its content to pass to any third party without the express permission of the Sponsor or Author.

Geographic Scope of this Document

This Policy applies to all Crawford operations.

Audience

Intended Audience	Intended Method of Distribution	Proposed Date
Crawford Employees and Contractors		