3 Phillip Street
13-03 Royal Group Building
Singapore 048693
www.trustsphere.com

Privacy Position Paper

TrustSphere Relationship Analytics for Sales

Roland Turner, Chief Privacy Officer.

October 27, 2016.

Executive Summary

Relationship Analytics for Sales improves the effectiveness of an organization's CRM by closing large gaps in the available information, using fully automated means to extract relevant information from the organization's existing communication/collaboration systems, without encroaching upon individual privacy. It only uses data legitimately available to the organization and uses the minimum sufficient amount of data to achieve this objective.

By design, all TrustSphere products and services respect individual privacy.

Relationship Analytics for Sales never analyzes the content of subject headers, message bodies, or email attachments. This limitation has been systematically imposed to secure the privacy of individual correspondents. Relationship Analytics for Sales surfaces connections and relationships between an employee and customers based on communication flows which have occurred using the corporate communication/collaboration servers only. It does not look at other network traffic or examine the firewall to understand personal traffic and therefore does not look at an individual’s personal email accounts or personal mobile devices.

This paper details the privacy implications of implementing Relationship Analytics for Sales and describes how compliance with the relevant requirements of various jurisdictional / territorial frameworks is maintained.

Any questions or clarifications may be addressed directly to the author at roland.turner@trustsphere.com.

Contents

.

Overview

Audience

This document is intended for use by those interested in or responsible for an organization's compliance with privacy legislation. This is typically those in the office of the Chief Privacy Officer, Chief Data Officer, and/or General Counsel.

Objective

This document should provide:

- an understanding of how Relationship Analytics for Sales works in combination with an organization's CRM,
- a high level understanding of the technology and data flows, and
- an understanding of why an implementation of Relationship Analytics for Sales is likely to be compliant with privacy legislation in operation in the organization's jurisdiction.

Description of TrustSphere Relationship Analytics for Sales

The Business Challenge

Relationship Analytics for Sales addresses a well known, industry-wide challenge for CRM deployments. CRM systems are an established category of technological solution deployed for the purpose of providing an organization with a shared, coordinated and comprehensive understanding of their current and prospective customers:

- In principle, a CRM makes all relevant customer-related activity available in one technology system, thereby allowing the organization to better serve its customers by providing the information needed to support a variety of customer-centric workflows (sales, customer support, renewals, licensing etc) in one place.
- In practice, most CRMs require that much of the necessary information be manually entered by sales representatives and customer facing teams which, experience has proved, typically does not occur.
- This leaves CRMs incomplete from a customer data perspective.

How Relationship Analytics for Sales Improves the Situation

Relationship Analytics for Sales automates:

- the extraction of relevant information from email and other communication/collaboration systems;
- transformation of that data into a form suitable for use in the CRM; and
- insertion of the transformed data into the CRM, or making it available for use there.

This goes some way toward completing the CRM with important and relevant data which allows an organization to serve its customers more effectively with greater collective knowledge.

Purposes Served

The improvements described above allow an organization to better pursue the following data processing purposes:

- Automatically finding and populating the CRM with many more customer contact points than have been manually entered in the system by sales teams. This provides the true contact base for the organization (completes the collective “address book”) without relying on or burdening sales teams for data entry, thereby improving the ability of sales teams to serve the organization’s customers.
- Accurately identifying those accounts, contacts or leads which are being ignored – using both the updates entered in the CRM and updates from the communication system, the latter not relying on data entry by the sales team – thereby enabling prompt intervention to sustain the strength of the relationship.
- Minimizing customer and revenue impact when transitioning accounts between sales team members as a more complete set of data is now available within the CRM.

Note that both Relationship Analytics for Sales and the broader TrustVault suite have a considerably larger range of capabilities than those discussed here. This paper only addresses implementations in which[1]:

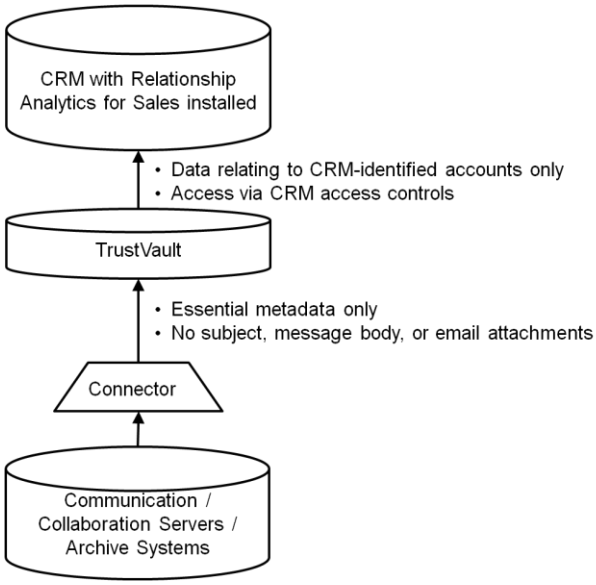
- subject header processing has not been switched on in any connectors in use, and
- data retention has not been set to an indefinite period.

The privacy impact of implementing additional capabilities or altering the prescribed settings is outside the scope of this paper.

[1] where the customer organization has control of these settings

Understanding Data Flow

These capabilities are achieved by processing metadata stored in the organization's existing communications systems.



At each stage of the process, the smallest reasonable subset of the available data is processed:

- Multiple distinct strategies are used to extract data from the organization's existing systems; the software components which implement these strategies are referred to as connectors. The connectors work with the smallest useful subset of the data made available by the interface in use, and then pass only essential metadata (usually: date and time, direction, sender, recipient, size) to TrustVault.
- Data that is inserted into, or made visible from, the CRM relates only to corporate communication with customers[2] identified in the CRM.
- Access to relationship analytics in the CRM follows the existing access control structure: only those users who already have access to information about a particular customer have access to relationship analytics about that customer.

[2] References to customers in this document also refer to prospects wherever it makes sense to do so.

Delivery

Relationship Analytics for Sales, TrustVault and the connectors can be delivered in either or both of two forms:

- as licensed software for execution on servers controlled by the customer organization whether on the customer's premises or elsewhere, described as "on premises"; or
- on a SaaS basis, described as "cloud".

Choice of Privacy Principles

As TrustSphere is a global organization, selecting a single jurisdiction's expression of its privacy principles as the basis for establishing, executing, and expressing our privacy stance is impractical. Fortunately, since 1980 the OECD has been promulgating a set of widely-agreed principles which are not specific to any single jurisdiction; TrustSphere uses these as the basis for establishing and describing our privacy stance internally and for communicating it externally. We then treat the more specific or restrictive obligations that exist in limited individual jurisdictions as important special cases that we address specifically.

Note that all of the quoted text and paragraph numbers in the definitions and in the individual principles come from the latest revision of The OECD Privacy Framework[3].

Definitions

> OECD PF (2013) 1. a) "Data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

In the context of a Relationship Analytics for Sales implementation, the data controller is the customer organization whose sales teams' communication metadata is being processed and in whose CRM the results are being presented.

Where Relationship Analytics for Sales is provided on a SaaS basis, TrustSphere is an agent acting as a data processor on the customer's behalf while the customer organization remains the data controller, in accordance with the principles and practices applicable to SaaS applications generally. As data controller, the customer organization always retains effective control of the data.

> OECD PF (2013) 1. b) "Personal data" means any information relating to an identified or identifiable individual (data subject).

[3]The latest revision was released in 2013 and can be found at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Note that this definition is as broad as possible and, in particular, has the effect of including metadata about communication performed by the organization's employees when communicating on behalf of that organization. Consequently, the conclusions of this analysis is valid across the entire range of definitions of personal or private data used by different jurisdictions.

OECD Principles

Collection Limitation

> OECD PF (2013) 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

As only metadata already legitimately possessed by the organization in its communication systems is processed, no new collection of personal data is performed and compliance with this principle is unaffected by implementation of TrustVault and Relationship Analytics for Sales.

Data Quality

> OECD-PF (2013) 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

The limited personal data used, namely metadata about communication between sales team members and employees of identified customer organizations, is directly relevant to each the purposes served.

Accuracy, completeness, and currency all result automatically from the fully automated, fully deterministic means used to extract metadata from the organization's existing communication systems, transform that data, and insert it into their CRM or make it available there:

- As the means of extracting the metadata is fully automated, there is no risk of human transcription error.
- As the means of extracting the metadata is fully deterministic, there is no risk of statistical uncertainty or errors in machine learning.

Purpose Specification

> OECD-PF (2013) 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Each of the purposes served falls unambiguously within the scope of the sales teams' work to conduct the organization's sales activities and the management of those teams, and therefore both:

- falls within the purpose of providing organizational communication systems to sales teams in the first place, and
- is a purpose compatible with the purpose of providing organizational communication systems to sales teams.

Use Limitation

> OECD-PF (2013) 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
>
> a) with the consent of the data subject; or
>
> b) by the authority of law.

As the purposes served both fall within and are compatible with the purposes of the collection of data by existing organizational communication systems, compliance with this principle is not affected.

Security Safeguards

> OECD-PF (2013) 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Relationship Analytics for Sales has access controls built in to limit access to identified individuals who have a legitimate need to know. It does so by respecting the access controls already built into the CRM system.

The implementation of these controls is dependent upon the security of the environment in which the software is running:

1) Where Relationship Analytics for Sales has been provided for “on premises” use, this security is entirely under the organization’s control and would ordinarily be expected to be comparable to the measures used by the organization to secure other data of comparable sensitivity in its possession.
2) Where Relationship Analytics for Sales has been provided by TrustSphere on a SaaS basis:
   a) TrustSphere applies commercially reasonable measures to protect the data as confidential customer data, including hosting only with tier 1 hosting providers. More details are provided in the TrustSphere Information Security Practices document.
   b) TrustSphere is contractually bound to process data in this situation on the basis that the controller (i.e. customer organization) always maintains effective control.

Openness

> OECD-PF (2013) 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

As this principle describes the stance of the organization with respect to personal data in its possession generally rather than anything to do with a specific tool, compliance with this principle is not affected.

Individual Participation

OECD-PF (2013) 13. Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

An organization can extract from Relationship Analytics for Sales at will any data stored relating to an identified individual. As this data is designed to be in a form that is intelligible to most users of TrustSphere's software, it can be supplied as-is in response to such a request.

There are no meaningful challenges to the data as:

- the data is extracted from the organization's communication systems automatically, without risk of human transcription error;
- the data is extracted from the organization's communication systems deterministically, meaning that there is no risk of statistical uncertainty or errors in machine learning; and
- there is no scope for any data alteration or amendment.

Accountability

> OECD-PF (2013) 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

This principle is not affected by an organization implementing and operating Relationship Analytics for Sales.

Additional Principles

TrustSphere adopts the following principle in processing personal data, over and above those recommended by OECD.

Data Minimization

TrustVault and Relationship Analytics for Sales process, store, and present the smallest useful subset of the data in use for the purposes described in this document:

- connectors disregard everything except essential metadata (in particular: subject headers, message bodies, and attachments are not processed),
- TrustVault stores only that essential metadata and analytics derived from it,
- only data relating to identified domains for identified customers in the CRM is stored or made available there, and
- CRM users are only provided with access to relationship information relating to customers that they have access to.

There are few or no situations in which data more than three years old is relevant for the purposes described in this document, consequently data exceeding this age is automatically purged regularly.

Conclusion

Compliance with each of the principles is either:

- completely supported, or
- entirely unaffected

by implementing and operating TrustSphere's TrustVault and Relationship Analytics Solutions for Sales.

Consequently an organization's compliance with its privacy obligations is not impacted by implementing and operating TrustVault and Relationship Analytics for Sales.

Appendix A – Jurisdiction-Specific Considerations

Singapore PDPA

The PDPA[4] generally permits:

- collection without consent of personal data "produced in the course, and for the purposes, of the individual's employment, business or profession; and collected for purposes consistent with the purposes for which the document was produced;" (17(1), Second Schedule 1(n));
- use without consent of "data was collected by the organisation in accordance with section 17(1), and is used by the organisation for purposes consistent with the purpose of that collection" (17(2), Third Schedule 1(j)); and
- disclosure without consent of data which "was collected by the organisation in accordance with section 17(1); and is disclosed by the organisation for purposes consistent with the purpose of that collection." (17(3), Fourth Schedule 1(s)).

As sales team email data and metadata are collected for the purpose of conducting the organization's sales function, and as the purposes described in this document are consistent with that purpose, an organization's implementation and use of Relationship Analytics for Sales complies with the collection, use and disclosure obligations of the PDPA.

[4] https://www.pdpc.gov.sg/legislation-and-guidelines/legislation

EU Directive 95/46/EC (Data Protection Directive)

Directive 95/46/EC creates obligations for controllers in Articles 6 through 19.

Article 6 - Principles relating to data quality

> "personal data must be ... (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"

Compliance is based upon adherence to the Purpose Specification principle.

> "(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;"

Compliance is based upon adherence to the Data Minimization principle.

> "(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;"

Compliance is based upon adherence to the Data Quality principle.

Article 7 - Criteria for making data processing legitimate

> "personal data may be processed only if: ... (f) processing is necessary for the purposes of the legitimate interests pursued by the controller"

The purposes described in this document are all legitimate interests of the controller.

Article 8 - The processing of special categories of data

Not applicable. TrustVault and Relationship Analytics for Sales are not used for these purposes.

Article 9 - Processing of personal data and freedom of expression

Not applicable. TrustVault and Relationship Analytics for Sales are not used for these purposes.

Article 10 - Information in cases of collection of data from the data subject

Not applicable. TrustVault and Relationship Analytics for Sales do not collect personal data.

Article 11 - Information where the data have not been obtained from the data subject

Not applicable. TrustVault and Relationship Analytics for Sales do not collect personal data.

Article 12 - Right of access

Compliance is based upon adherence to the Individual Participation principle above

Article 13 - Exemptions and restrictions

Not applicable. TrustVault and Relationship Analytics for Sales are not used for these purposes.

Article 14 - The data subject's right to object

Compliance is based upon adherence to the Individual Participation principle above.

Article 15 - Automated individual decisions

Not applicable. TrustVault and Relationship Analytics for Sales are not used for these purposes.

Article 16 - Confidentiality of processing

This is largely an obligation upon a controller to contractually limit the activities of employees and controllers, however:

- the access control mechanisms in Relationship Analytics for Sales support implementation of this obligation in that data relating to a particular account is only disclosed to people who are already recognized by the CRM as having right of access to information about that account, and
- where TrustVault and/or Relationship Analytics for Sales are provided on a SaaS basis, TrustSphere operates as a processor under the direction of the controller; the controller always retains effective control.

Article 17 - Security of processing

Compliance is based upon adherence to the Security Safeguards principle above.

Articles 18 and 19 - Obligation to notify the supervisory authority, Contents of notification

Where member state law requires notification of processing of stored communications for purposes consistent with its collection, existing notifications would ordinarily already cover the purposes described in this document.

EU Regulation 2016/679 (General Data Protection Regulation)

GDPR imposes obligations on data controllers in Articles 5 through 22. Articles 44 through 50 are also worthy of comment given TrustSphere's being based in Singapore.

Article 5 - Principles relating to processing of personal data

> "1. Personal data shall be: ... (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"

Compliance is based upon adherence to the Purpose Specification principle.

> "(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');"

Compliance is based upon adherence to the Data Minimization principle.

> "(d) accurate and, where necessary, kept up to date"

Compliance is based upon adherence to the Data Quality principle.

> "(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;"

Compliance is based upon adherence to the Data Minimization principle.

> "(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Compliance is based upon adherence to the Security Safeguards principle.

Article 6 - Lawfulness of processing

> "1. Processing shall be lawful only if ... (f) processing is necessary for the purposes of the legitimate interests pursued by the controller"

> "4. Where the processing for a purpose other than that for which the personal data have been collected ... the controller shall ... take into account, inter alia:"

Compliance is based upon adherence to the Purpose Specification principle.

Article 7 - Conditions for consent

Not applicable. Processing occurs without additional consent under the terms of Article 6 paragraphs 1(f) and 4.

Article 8 - Conditions applicable to child's consent in relation to information society services

Not applicable. Personal data relating to children is not relevant in a B2B context.

Article 9 - Processing of special categories of personal data

Not applicable. TrustVault and Relationship Analytics for Sales are not used for processing data of this type.

Article 10 - Processing of personal data relating to criminal convictions and offences

Not applicable. TrustVault and Relationship Analytics for Sales are not used for processing data of this type.

Article 11 - Processing which does not require identification

Not applicable. Most TrustVault and Relationship Analytics for Sales processing requires identification.

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject

Not applicable. These are procedural obligations of the controller that are not altered by the implementation and use of TrustVault and Relationship Analytics for Sales.

Article 13 - Information to be provided where personal data are collected from the data subject

Not applicable. TrustVault and Relationship Analytics for Sales do not collect personal data.

Article 14 - Information to be provided where personal data have not been obtained from the data subject

Not applicable. TrustVault and Relationship Analytics for Sales do not collect personal data.

Article 15 - Right of access by the data subject

Compliance is based upon adherence to the Individual Participation principle.

Article 16 - Right to rectification

Not applicable. Compliance is based upon adherence to the Individual Participation principle.

Article 17 - Right to erasure ('right to be forgotten')

Not applicable. Compliance is based upon adherence to the Individual Participation principle.

Article 18 - Right to restriction of processing

Not applicable. Compliance is based upon adherence to the Individual Participation principle.

Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing

Not applicable. Compliance is based upon adherence to the Individual Participation principle.

Article 20 - Right to data portability

Compliance is based upon adherence to the Individual Participation principle.

Article 21 - Right to object

Not applicable. Compliance is based upon adherence to the Individual Participation principle.

Article 22 - Automated individual decision-making, including profiling

Not applicable. TrustVault and Relationship Analytics for Sales are not used for decisions of this type.

Article 23 - Restrictions

Not applicable. TrustVault and Relationship Analytics for Sales are not used for these purposes.

Article 24 - Responsibility of the controller

Not applicable. These are general procedural obligations of the controller.

Article 25 - Data protection by design and by default

Compliance is based upon adherence to the Security Safeguards, Data Quality and Data Minimization principles.

Article 26 - Joint controllers

Not applicable. TrustVault and Relationship Analytics for Sales are not used in situations of this type.

Article 27 - Representatives of controllers or processors not established in the Union

With respect to the organization's role as a controller: implementing and using TrustVault and Relationship Analytics for Sales does not create any new obligations.

With respect to TrustSphere's role as a processor (where Relationship Analytics for Sales has been provided for use on a SaaS basis): such a designation will be made before the Regulation comes into effect in 2018.

Article 28 - Processor

TrustSphere's terms of service will be amended to suit before the Regulation comes into effect in 2018.

Article 29 - Processing under the authority of the controller or processor

Compliance is based upon adherence to the Security Safeguards principle.

Article 30 - Records of processing activities

The formal creation and retention of records in the prescribed format will be implemented before the Regulation comes into effect in 2018.

Article 31 - Cooperation with the supervisory authority

TrustSphere's terms of service will be amended to suit before the Regulation comes into effect in 2018.

Article 32 - Security of processing

Compliance is based upon adherence to the Security Safeguards principle.

Article 33 - Notification of a personal data breach to the supervisory authority

TrustSphere's breach response process will be updated to suit before the Regulation comes into effect in 2018.

Article 34 - Communication of a personal data breach to the data subject

TrustSphere's breach response process will be updated to suit before the Regulation comes into effect in 2018.

Articles 35 and 36 - Data protection impact assessment and prior consultation

Not applicable. TrustVault and Relationship Analytics for Sales are not used for processing data of this type.

Articles 37 through 39 - Data protection officer

TrustSphere will complete implementation of these requirements before the Regulation comes into effect in 2018.

Articles 44 through 50 - Transfers of personal data to third countries or international organisations

Not applicable:

- Where TrustVault and/or Relationship Analytics for Sales has been provided for use on a SaaS basis, all processing is performed in the United Kingdom.
- Where TrustVault and/or Relationship Analytics for Sales has been provided for "on premises" use, these articles create no new obligations.

USA - Federal

US Federal law includes the following with subject matter related to TrustVault and Relationship Analytics for Sales.

Electronic Communications Privacy Act of 1986 § 2701-2711.

> "(a) Offense.—Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;"

Not applicable. TrustVault and Relationship Analytics for Sales operate entirely on the basis of authorized access.

Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code section 6501 and following

Not applicable. Personal data relating to children is not relevant in a B2B context.

USA - California

In addition to federal laws, California state law includes the following with subject matter related to TrustVault and Relationship Analytics for Sales.

Data Breach Notice - California Civil Code sections 1798.29 and 1798.82.

> "1798.82 (h)(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account."

Not applicable. Although TrustVault and Relationship Analytics for Sales process email addresses, they do not also process passwords or security questions or answers.

Security of Personal Information - California Civil Code section 1798.81.5.

> "1798.81.5 (d)(1)(B) A username or email address in combination with a password or security question and answer that would permit access to an online account."

Not applicable. Although TrustVault and Relationship Analytics for Sales process email addresses, they do not also process passwords or security questions or answers.

Were this Code section to be broadened to include email addresses on their own, compliance would addressed as described in the Security Safeguards principle.

Workplace Surveillance - California Labor Code section 435

> "435. (a) No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order."

Not applicable. This Code section deals narrowly with recordings of the type described above only.

USA - New York

In addition to federal laws, New York state law includes the following with subject matter related to TrustVault and Relationship Analytics for Sales.

General Business Law 899-aa. Notification; person without valid authorization has acquired private information

> "899-aa 1. (b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:
>
> (1) social security number;
>
> (2) driver's license number or non-driver identification card number; or
>
> (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;"

Not applicable. TrustVault and Relationship Analytics for Sales do not process information of this type.

Labor Law 203-d. "Employee personal identifying information …"

> "203-d(d) Communicate an employee's personal identifying information to the general public. For purposes of this section, "personal identifying information" shall include social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number."

Not applicable. Although 203-d(d) refers to email addresses, TrustVault and Relationship Analytics for Sales are not used for public disclosure of this information.

Australian Privacy Principles 2014

References are to the Australian Privacy Principles[5] as at January 2014 and the Australian Privacy Principles Guidelines 1 April, 2015[6]

APP 1 — open and transparent management of personal information

Not applicable. This describes the organization's compliance, independent of any particular collection, use, or disclosure of information.

APP 2 — anonymity and pseudonymity

Not applicable. TrustVault and Relationship Analytics for Sales do not operate on personal matters.

APP 3 — collection of solicited personal information

Not applicable. TrustVault and Relationship Analytics for Sales do not collect information.

APP 4 — dealing with unsolicited personal information

Not applicable. TrustVault and Relationship Analytics for Sales do not collect information.

APP 5 — notification of the collection of personal information

Not applicable. TrustVault and Relationship Analytics for Sales do not collect information.

APP 6 — use or disclosure of personal information

As the purposes described in this document are consistent with the reasonable expectations of sales team employees with respect to the purpose of the collection of stored communications data and metadata, 6.2(a)(ii) applies:

> "personal information about an individual if ... the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is ... related to the primary purpose"

APP 7 — direct marketing

Not applicable. TrustVault and Relationship Analytics for Sales are not used for direct marketing.

---

[5] https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

[6] https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf

APP 8 — cross-border disclosure of personal information

Where TrustVault and/or Relationship Analytics for Sales are supplied for "on premises", use, cross-border issues are entirely in the customer's control.

Where TrustVault and/or Relationship Analytics for Sales are supplied on a SaaS basis, TrustSphere processes the customer's information entirely under the customer's control, meaning that Guideline B.144 is applicable:

> "providing personal information to a contractor to perform services on behalf of the APP entity [is] a use rather than a disclosure ... where the entity does not release the subsequent handling of personal information from its effective control"

APP 9 — adoption, use or disclosure of government related identifiers

Not applicable. TrustVault and Relationship Analytics for Sales do not use government-related identifiers.

APP 10 — quality of personal information

Compliance is based upon adherence to the Data Quality principle above.

APP 11 — security of personal information

Compliance is based upon adherence to the Security Safeguards principle above.

APP 12 — access to personal information

Compliance is based upon adherence to the Individual Participation principle above.

APP 13 — correction of personal information

Compliance is based upon adherence to the Individual Participation principle above.

Disclaimer

This paper represents TrustSphere's position on the privacy implications of the use of TrustVault and Relationship Analytics for Sales for the purposes described in this paper. This is not legal advice; customers are advised to seek their own legal advice where appropriate.