

# PRIVACY AND DATA PROTECTION POLICY

## APEX SENTINEL GROUP PTY LTD

# TABLE OF CONTENTS


| | | |
|---|---|---|
| 1. | INTRODUCTION | 3 |
| 2. | PRIVACY AND DATA PROTECTION OF PERSONAL DATA | 3 |
| 3. | DEFINING PERSONAL DATA | 3 |
| 4. | SPECIAL CATEGORIES OF PERSONAL DATA | 6 |
| 5. | PROCESSING PERSONAL DATA | 6 |
| 6. | SHARING YOUR DATA | 8 |
| 7. | STORING YOUR DATA | 9 |
| 8. | PROCESSING PERSONAL DATA FOR APEX | 9 |

# 1. INTRODUCTION

1.1 Apex Sentinel Group Pty Ltd (Apex) takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act'), the EU General Data Protection Regulation ('GDPR') and the Australian Privacy Act 1988 ('Privacy Act 1988') in respect of data privacy and security. We have to notify you of the information contained in this policy.

1.2 This policy applies to current and former team members, workers, volunteers, apprentices, and consultants. Additionally, it applies to any client, website visitor, partners, or external stakeholder who interacts with Apex Sentinel: specifically, those who provide sensitive and personal data. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time concerning your data.

1.3 Apex is a 'data controller' for your data. This means that we determine the purpose and means of the processing of your data.

1.4 This policy explains how Apex will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, Apex

1.5 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by Apex at any time. It is intended that this policy is fully compliant with the Data Protection Act 2018, GDPR and the Privacy Act 1988. If any conflict arises between those laws and this policy, Apex intends to comply with the 2018 Act, GDPR and the Privacy Act 1988.

# 2. PRIVACY AND DATA PROTECTION OF PERSONAL DATA

2.1 Personal data must be processed by six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

2.2 We are accountable for these principles and must be able to show that we are compliant.

# 3. DEFINING PERSONAL DATA

3.1 'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information about your tax status including your national insurance number;
- your identification documents including passport and driving licence and information about your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information concerning your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video) and
- any other category of personal data which we may notify you of from time to time.

## 4. SPECIAL CATEGORIES OF PERSONAL DATA

4.1 'Special categories of personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

4.2 We may hold and use any of these special categories of your data under the law.

## 5. PROCESSING PERSONAL DATA

5.1 Apex will process your data (including special categories of personal data) following our obligations under the 2018 Act, Privacy Act 1988 and GDPR.

5.2 We will use your data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs).

5.3 We can process your data for these purposes without your knowledge or consent. We will not use your data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

5.4 If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC/ATO or to make reasonable adjustments concerning any disability you may suffer from.

5.5 We have to process your data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement). For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure about you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of Apex, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits under the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend Apex in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time. *see point 3.8

5.6 We will only process special categories of your data (see above) in certain situations under the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request.

- We do not need your consent to process special categories of your data when we are processing it for the following purposes, which we may do:
- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for occupational medicine or the assessment of your working capacity.

5.7 We will process information about criminal convictions if this is necessary for the provision of our services to a client or group of clients (e.g. schools).

5.8 We might process special categories of your data for the purposes in point 3.5 above which have an asterisk beside them. In particular, we may use information concerning:

- your race, ethnic origin, orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

5.9 We do not take automated decisions about you using your data or use profiling concerning you. If this changes, we will notify you.

## 6. SHARING YOUR DATA

6.1 Sometimes we might share your data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

6.2 We require those companies to keep your data confidential and secure and to protect it following the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and following our instructions.

6.3 We use contractors as data processors for these functions:

- HR consultancy

- Data protection consultancy
- Pension
- Accountancy
- Legal advice

6.4 We do not send your data outside the European Economic Area or Australia. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

6.5 When there is a requirement to share your data, Apex will share via secure and encrypted mechanisms to ensure data integrity and accountability.

## 7. STORING YOUR DATA

7.1 Apex uses various cloud (SaaS) technologies to store your data. These systems have the following security controls in place:

- Multi-Factor / 2-Factor Authentication
- Encryption
- Role-based access
- Auditing

7.2 Data downloaded and stored at rest on Apex computers will also be protected via disk encryption mechanisms.

7.3 Apex will monitor and audit the above security mechanisms. It is also the responsibility of all team members processing sensitive information to ensure these mechanisms are active for their accounts and devices respectively. If any of the above security services are inactive or malfunctioning, this should be reported to management immediately.

## 8. PROCESSING PERSONAL DATA FOR APEX

8.1 Everyone who works for, or on behalf of Apex has some responsibility for ensuring data is collected, stored and handled appropriately.

8.2 Apex‘s Chief Operations Officer is responsible for reviewing this policy and updating the Director on Apex’s data protection responsibilities and any risks concerning the processing of data. You should direct any questions about this policy or data protection to this person.

8.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of Apex and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

8.4 You should not share personal data informally.

8.5 You should keep personal data secure and not share it with unauthorised people.

8.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your contact details change.

8.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

8.8 You should use strong passwords.

8.9 You should lock your computer screens when not at your desk.

8.10 Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

8.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

8.12 Do not save personal data to your personal computers or other devices.

8.13 Personal data should never be transferred outside the European Economic Area and Australia except in compliance with the law and authorisation of the Director.

8.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

8.15 You should not take personal data away from Apex 's premises without authorisation from the Primary Security Officer, Chief Operations Officer or Director.

8.16 Personal data should be shredded and disposed of securely when you have finished with it.

8.17 You should ask for help from your team and then the Chief Operations Officer, or Director. If you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

8.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you following our disciplinary procedure.

8.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

8.20 Dealing with data breaches

8.21 We have robust measures in place to minimise and prevent data breaches from occurring.

8.22 Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office, UK/Office of the Australian Information Commissioner within 72 hours.

8.23 If you are aware of a data breach you must contact the Primary Security Officer, Chief Operations Officer or Director immediately and keep any evidence, you have concerning the breach.

8.24 Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Chief Operations Officer or Director. who will coordinate a response.

8.25 If you would like to make a SAR about your data, you should make this in writing to the Chief Operations Officer or Director. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

8.26 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

8.27 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

8.28 You have the right to access your data by way of a subject access request (see above).

8.29 You can correct any inaccuracies in your data.

8.30 You have the right to request that we erase your data where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected.

8.31 While you are requesting that your data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made.

8.32 You have the right to object to data processing where we are relying on a legitimate interest to do so, and you think that your rights and interests outweigh our own and you wish us to stop.

8.33 You have the right to object if we process your data for direct marketing.

8.34 You have the right to receive a copy of your data and to transfer your data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

8.35 With some exceptions, you have the right not to be subjected to automated decision-making.

8.36 You have the right to be notified of a data security breach concerning your data.

8.37 In most situations, we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your data for a specific purpose, you have the right not to consent or to withdraw your consent later.

8.38 To exercise any of the rights above please contact the Chief Operations Officer or Director.

8.39 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office in the UK or the Office of the Australian Information Commissioner directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk or www.oaic.gov.au ). This website has further information on your rights and our obligations.

FOR FURTHER ASSISTANCE,
PLEASE CONTACT THE APEX TEAM.

APEX SENTINEL GROUP

TEL: +61 (0)413 322 874
ENGAGEMENT@APEXLOGIC.COM.AU

APEXSENTINEL.COM.AU