PRIVACY POLICY – AUSTRALIA

Including Data Breach Reporting

Status:	Final
Version:	1
Policy Owner:	General Manager Seeds Australia
Policy Approver:	Group General Manager Seed & Grain
Date:	21 December 2017

Privacy Policy

Purpose	The Privacy policy covers how PGG Wrightson Seeds (Australia) Pty Ltd including Auswest and Stephen Pasture Seeds (PGW) will manage individual customer, employee and third party information and data breaches to ensure compliance with the Privacy Act.
Key Points	This policy covers: • What we collect, and why • How we collect it • Where we store it • What we can use it for • Who can we disclose it to • Data quality and security • Communication • Our Websites
Scope	PGG Wrightson Group – Australian Operations
Date of issue	22 November 2017
Availability	This policy is available on the PGG Wrightson Seeds Australia Websites, or you can request a copy by contacting PGG Wrightson Seeds Pty Ltd Commercial Manager on +61 3 8379 7435.
Review	This policy is reviewed every 2 years by General Manager Strategy & Corporate Affairs with input from General Managers.

Related Policies and Documents

Privacy Act	*Privacy Act 1988 (Cth)* including the Australian Privacy Principles - external site.
Code of Conduct	http://pggwrightson.co.nz/our-company/investors/governance

1. Policy Standard

1.1 Purpose

This policy explains how PGW will manage all personal information in accordance with the Privacy Act.

PGW is committed to ensuring the privacy of personal information is protected and we strive to uphold the best practice privacy standards in the collection, storage and use of personal information.

1.2 Definitions

Personal Information means any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not'.

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

Sensitive information is a subset of personal information and is defined as:

- information or an opinion (that is also personal information) about an individual's:
    - racial or ethnic origin
    - political opinions
    - membership of a political association
    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual orientation or practices, or
    - criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates.

Sensitive information is generally afforded a higher level of privacy protection than other personal information.

1.3 Scope

This Privacy Policy applies to personal information held about individuals. The Privacy Act and this Privacy Policy do not apply to information we hold about companies and other organisations as they are not identifiable individuals covered by the Privacy Act. However PGW does keep completely confidential all information that we hold about companies and other organisations regarding their strategies, business affairs, accounts, finance or contractual arrangements.

This Privacy Policy covers Australian:

- PGW customers, suppliers and third parties;
- Directors and Officers of PGW Group Companies;
- Employees (full time and part time);
- Temporary and Casual employees;
- Independent contractors
- Third party contractors e.g. consultants; and

1.4 What we collect, and why

Personal information collected by PGW is collected for the purpose of managing customer transactions for products and services, supplier and other third party relationships, and employee relationships.

The personal information we collect differs depending on which of our products and services you are involved in, and may include:

- name, address and contact details
- date of birth
- gender
- account and newsletter preferences
- for employees, all employment related information
- for customers, information about a product or service you purchased from or sold to us, the place of purchase and information about your ownership of the product
- information about any call to us, including a recording of the call, details about the product(s) you bought, the reason why you contacted us and the advice we gave you
- information relating to your use of any of our loyalty programs and the rewards that you claim
- information about third party provider products that you obtain through us eg fuel cards
- your business contact details and other business information, place of employment and position
- product reviews, comments, photos and forum posts that you have submitted;
- credit and financial information and checks, including validation of identity and property ownership
- information about your social network profile such as your social network ID, profile picture, gender and location
- the fact that you have clicked on a 'like' or 'tweet' or similar button in one of our websites or services or one of our pages on a social network site, which we may associate with the details that we store about you
- information about your visit to our website, such as your browser software, which pages you view and which items you 'clicked' on
- service, product or server logs, which hold technical information about your use of our service, product or websites, such as your IP address, domain, device and application settings, errors and hardware activity
- information about where your device is physically located (for example, when you are using a geo-location service or application and you have provided consent to your location being shared)
- interests and preferences that you specify during setup of an Internet enabled product or service
- in the case of candidates seeking employment with us, and our employees, information relevant to your employment history.

If we request personal information from you and you do not supply it, we may not be able to provide you with the product or service you request. We also sometimes collect information about people who are not our employees or customers as part of providing a product or service, for example the other party to a sales transaction that you are involved in.

PGW only collects sensitive information (eg health information) where it is reasonably necessary for our functions or activities and either you have consented, or we are required or authorised by law to do so. Generally sensitive information such as health information would only be collected about our staff where necessary.

1.5 How we collect it

Whenever possible, we collect personal information directly from you. Collection occurs when you first apply or request a product or service from us or start work with us, also during the course of our relationship with you we may continue to collect personal information. Information may be collected in various ways, such as mail, internet, telephone, face to face conversation, email, and in various formats such as forms, letters, electronic file notes and recorded conversations. Customers will be identified by a PGW customer number and password (if applicable). Employees will be identified by a PGW employee number and password (where applicable).

We may also collect personal information from other people, organisations and sources, such as when collection from you is impractical or where you have consented to us collecting it from someone else. These may be parties related to PGW or third parties such as your agent, where you have appointed an agent to act on your behalf in dealings with us (e.g. a broker or lawyer), or employment referees that prospective employees have given us.

1.6 Where we store it

PGW stores customer and employee personal information in a number of locations, including:

- customer and employee documentation is scanned into PGW's computer systems, various equipment, programmes, databases and digital archives
- physical paperwork is filed in a secure location
- electronic files are stored securely with third party cloud-hosting providers

These storage mechanisms may be managed internally by PGW and held locally in New Zealand, or they could be managed by a third party storage provider with whom PGW has a contractual relationship and be held on a server locally or overseas.

1.7 What we can use it for

Personal information will be used by PGW in association with any past or future sales, transactions, interactions or proposals between PGW and the customer or employee including to:

- identify you when you telephone us to make an enquiry. For example, we may ask for your date of birth so that we can avoid disclosing information to a person who is not authorised by you to receive it
- contact you about any services and products provided by us previously, now or in the future
- help prevent or detect fraud or loss
- contact you by any means (including mail, email or telephone) in relation to a particular service or product
- contact you for research/feedback purposes
- make changes to your PGW account details

- provide you with a product or service you have requested, including checking that a payment is not made fraudulently, delivering your purchase to you or ensuring that you benefit from any relevant special offer or promotion
- train staff and for quality assurance purposes
- obtain opinions or comments about PGW products and/or services, including conducting product surveys
- respond to your requests for information when you contact us about PGW and its products and services
- conduct prize draws, contests and other promotional offers
- consider employing you if you contact us via one of PGW's job application websites
- record statistical data for marketing analysis
- manage employee information, including using it for human resources, payroll and health and safety matters, and data-matching.

This may include disclosure to our overseas related companies within the PGG Wrightson Group in New Zealand, South America and other counties.

1.8 Who can we disclose it to

PGW will not give personal information to a third party unless authorised under the Privacy Act.

In general, PGW does not sell, rent or otherwise disclose information about you to third parties without your consent. However, there are exceptions. PGW may disclose your personal information to third party service providers so that they can provide certain contracted services to PGW, such as IT support or programming, hosting services, telephony services, fulfilling orders, delivering packages, mailing or sending of documents to you electronically or otherwise, processing payments and providing fraud checking services.

We prepare anonymous, aggregate or generic data (including "generic" statistics) for a number of purposes, including for product and service development, business promotion and research purposes. As we consider that this is not personal information, we may share it with any third party (such as our suppliers, advertisers, industry bodies, the media and/or the general public).

1.9 Data Quality and Security

PGW will not use any personal information about our customers or employees without taking reasonable steps to ensure that the information is up to date, complete, relevant and not misleading.

Please take care when submitting personal information to us, in particular when completing free text fields or uploading documents and other materials. Some of our services are automated and we may not recognise that you have accidentally provided us with incorrect or sensitive information.

If you believe that any of the personal information that we hold about you is not accurate, complete or up-to-date, please let us know.

PGW will take all reasonable steps to store your personal information safeguarding against loss, misuse and disclosure, such as:

- following certain procedures, for example checking your identity against available data when you telephone us and using secure passwords for our computer systems
- limiting physical access to PGW’s premises

- limiting access to personal information to those who specifically need it to conduct their business responsibilities
- requiring our third party providers to have acceptable security measures to keep personal information secure
- putting in place physical, electronic, and procedural safeguards in line with industry standards; and
- destroying personal information pursuant to the law and our record retention policies.

PGW cannot guarantee that your personal information cannot be accessed by an unauthorised person (e.g. a hacker) or that unauthorised disclosures will not occur. If we provide you with any passwords or other security devices it is important that you keep these secret and confidential and do not allow them to be used by any other person. Please notify us immediately if the security of these devices is breached.

1.10 Access and Correction

We will generally provide you with access to your personal information within 30 days, subject to some exceptions permitted by law. We will also generally provide access in the manner that you have requested (eg by providing photocopies or allowing a file to be viewed), provided it is reasonable and practicable for us to do so. We may however charge a fee to cover our reasonable costs of locating the information and providing it to you.

If you ask us to correct personal information that we hold about you, or if we are satisfied that the personal information we hold is inaccurate, out of date, incomplete, irrelevant or misleading, we will take reasonable steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading. If we correct personal information about you, and we have previously disclosed that information to another agency or organisation that is subject to the Privacy Act, you may ask us to notify that other entity. If so, we will take reasonable steps to do so, unless this would be impracticable or unlawful.

1.11 Communication

PGW may use your information to provide you with newsletters and other communications by post, email, telephone, social media and/or text message and through PGW apps, if you have provided your prior consent or we are otherwise permitted to do so under applicable law.

You can change your marketing communication preferences at any time:

- if you would like to unsubscribe from an email sent to you, follow the 'unsubscribe' link and/or instructions placed (typically) at the bottom of the email. But note that:
- if you use more than one e-mail address to contact PGW, you will need to unsubscribe separately for each email address; and
- this method will only unsubscribe for the newsletter or other communication that you have received and you should use one of the other methods if you wish to opt-out of all our marketing communications,
- you can contact us in order to change your marketing communication preferences.

If you provide us with an email address or phone number, you consent to electronic communication such as notices or reminders being sent to you via that address or number.

PGW may monitor and record communications we receive, including recording and storing phone calls. This may be done for quality and training purposes to improve the service that we provide, to ensure compliance with our practices and procedures and/or to provide evidence of a transaction such as where a contract is entered into, or a claim is made.

1.12 Our websites

From time to time, PGW may enable third parties to advertise on its websites. If the link is followed to the third party website from the PGW website, the website privacy policy of that third party applies, and PGW accepts no liability for breaches of privacy once such a link has been followed.

PGW's websites collect the domain names, not the email addresses of visitors. Our web server may require you to place a "cookie" (small data file) on your computer's hard drive, in order to track statistical information about navigation to and throughout certain areas of the site. If you are just surfing and reading information on our website, then we collect and store the following information about your visit:

- the IP address of your machine when connected to the Internet and the domain name from which you are accessing the Internet
- the operating system and the browser your computer uses, and any search engine you are using
- the date and time you are visiting
- the URLs of the pages you visit
- if you provide it, your email address

We use that information to measure the number of visitors to different parts of the site and, for example, to measure the effectiveness of advertising. Although we may publish aggregated information about usage patterns, we do not disclose information about individual machines except for the reasons set out below in this section. We do not sell information which identifies you personally. We may gather more extensive information if we are concerned, for example, about security issues. If necessary, we can disclose information to relevant law enforcement authorities.

Some of our online services may allow you to upload and share messages, photos, video and other content and links with others and/or create a publically accessible profile for your account. For example:

- the communities and forums area of our websites, allows you to post comments (with your account name), which are visible to other users of that service; and
- other services allow you to share a link which if clicked on may allow the recipient to access your uploaded content.

You should not expect any information that you make available to others via PGW's online services to be kept private or confidential. Content and links that you share might, for instance, be forwarded by your recipients to others. You should always exercise discretion when using such services.

2. Clarification and Breaches

2.1 Clarification

Further clarification of this policy can be obtained from PGG Wrightson Seeds Pty Ltd Commercial Manager on +61 3 8379 7435. We may amend this Privacy Policy from time to time. The current version will be posted on our website and a copy may be obtained by contacting us on +61 3 8379 7400.

2.2 Breaches of policy

If you want to report a suspected breach of your privacy or you do not agree with a decision regarding access to your personal information, please contact us. We have an internal complaints process to address such issues and will promptly acknowledge and investigate complaints.

Any enquires or complaints can be made direct to the PGW manager outlined in section 2.1.

We expect our procedures will deal fairly and promptly with your complaint.

2.3 Data Breaches

From 22 February 2018, we must notify data breaches as set out below.

A **data breach** occurs when personal information held by PGW is lost or subjected to unauthorised access or disclosure.

Examples of a **data breach** include when:

- a device containing customers' personal information is lost or stolen, or
- a database containing personal information is hacked, or
- personal information is mistakenly provided to the wrong person.

Not all data breaches are notifiable.

A **notifiable data breach or eligible data breach** is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

If PGW has reasonable grounds to **believe** an **eligible data breach** may have occurred:

- legal advice must be obtained.
- PGW must promptly notify the Office of the Australian Information Commissioner (OAIC) and any potentially affected individuals – follow the Eligible Data Breach Statement Requirement Section below.

PGW will also immediately:

- Alert all Directors.
- Immediately contact our firewall provider to attempt to block a repeat breach and identify the extent of data accessed.
- Alert internal users of those PGW systems affected and require passwords be reset.
- Action any other remedial action that will reduce or stop the risk of serious harm eg freezing accounts, remote wiping of devices and having accidental recipients delete or return data.

If PGW has reasonable grounds to **suspect** an **eligible data breach** may have occurred, the notification obligation does not immediately arise and:

- legal advice must be obtained.

- PGW will undertake a reasonable and expeditious assessment into the relevant circumstances within a maximum of 30 days. Where compliance with the 30 day limit is not possible, must document the reasons for the delay in a manner which demonstrates that we have taken all reasonable steps to complete the assessment within 30 days.

- PGW's GM Seeds Australia will lead the assessment and determine the investigative steps to be taken
- The assessment process and its outcome will be documented so as to assist in any future review of the steps taken. This will be particularly important if the outcome of the assessment is that no "eligible data breach" has occurred.
- If the assessment finds that an **eligible data breach** may have occurred we must promptly notify the Office of the Australian Information Commissioner (OAIC) and any potentially affected individuals – follow the **Eligible Data Breach Statement Requirements** Section below.

Eligible Data Breach Statement Requirements
PGW's notification Statement must include:

- PGW's contact details
- a description of the data breach
- the kinds of information concerned; and
- recommendations about the steps individuals should take in response to the data breach.

Identifying Breaches
PGW does not employ software to interrogate whether a breach has occurred, but instead relies on the PGW "firewall" and also that the systems where this information is held require individual login to mitigate risk. A breach is likely to be identified by our firewall provider, or when it enters the public arena. PGW will continue to monitor whether a more systematic way to identify breaches is possible.

PGW has an internal Privacy awareness on-line training course available to all staff. In addition training on identifying and notifying data breaches will take place.