

PRIVACY POLICY

Stock in the Channel



0333 772 0003

privacy@stockinthechannel.com

1-6 Yarmouth Place Mayfair London W1J7BU England



Stock in the Channel

Policy Documentation Authorisation

Document Identity Stock Channel Ltd Privacy Policy

Number Version 3.2

Signature *Paul Meyers*

Prepared by Paul Meyers

Approved by the Board 24/05/2018

Policy Operational from 24/05/2018

Disclaimer

Even though this document has been prepared with great care based on our understanding of the information provided, minor errors, omissions and deviations from the actual software and systems solution cannot always be avoided. The user therefore cannot derive any rights from the description and responses that follow. This document remains the property of Stock Channel Ltd.

Copyright ©2018 Stock Channel Ltd

All rights reserved. This document is supplied on the strict understanding that it is not to be copied or supplied in part or in whole to third parties without the prior written consent of:

Stock Channel Ltd
1-6 Yarmouth Place
Mayfair
London
W1J 7BU

0333 772 0003

Contents

Introduction	4
Why this policy exists.....	4
Personal Data We Collect.....	6
User Access Data.....	6
End Customer Data.....	6
Right to be forgotten.....	8
Procedure to request to <i>'be forgotten'</i>	8
Measurable outcome of being forgotten	8
Allowing users to edit their profile personal information	9
Data Portability – Subject Access Request.....	9
Procedure to submit a Subject Access Request	9
Measurable outcome of a subject access request	10
Personal Data Use & Storage	11
Staff responsibilities.....	11
Staff with Key Responsibilities.....	11
General guidelines for all staff	12
Data storage	12
Data use	13
Data accuracy.....	14

Introduction

Why this policy exists

Your privacy, and protecting it is important to us.

In order to provide our services, Stock Channel Ltd needs to collect and process information about some individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. Stock Channel Ltd operates under the familiar name of Stock in the Channel and www.stockinthechannel.com. References in this policy to Stock Channel Ltd refer to our services, products, apps, websites and servers.

This policy describes what personal data is collected, handled and stored, how we protect your data as we work with it, and how we comply with the law through the company's data protection standards.

This data protection policy ensures Stock Channel Ltd;

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.

Statement

GDPR stands for General Data Protection Regulation and replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and comes into effect on 25th May 2018. GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that individuals data is not processed without their knowledge and are only processed with their 'explicit' consent. GDPR covers personal data relating to individuals.

Stock Channel Ltd is committed to protecting the rights and freedoms of individuals with respect to the processing of personal data. GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

Paul Meyers

Paul Meyers, Director and Data Protection Officer.
May 10th, 2018.

Stock Channel Ltd, Registered in England, number 07083121,
Registered office: 1-6 Yarmouth Place, London, Greater London, W1J 7BU
Incorporated: 21 November 2009

Personal Data held by Stock Channel Ltd

Personal Data We Collect

By necessity, Stock Channel Ltd needs to store some personal information. There are two sets of data held; User Access Data and End Customer Data.

User Access Data

Every person who wishes to use Stock Channel Ltd needs to register and login. During the registration process, we collect the following personal data;

- Title
- First Name
- Last Name
- Telephone Number
- Email Address
- Business Name and Address
- Job Title

This data is collected in order to validate that the registered user is a legitimate trade professional, and to be able to identify who the person using the site is. We store the data permanently. The reason for doing so is so that users can log on and access the service easily. The names and other details of the site's users are not passed on to any third party.

End Customer Data

Stock Channel Ltd provides services to Client businesses who may sell, via Stock Channel Ltd, products to individuals. In order to be able to sell and deliver a product to that End Customer, it is necessary for Stock Channel Ltd to collect the following personal data;

- Title
- First Name
- Last Name
- Personal Email Address
- Telephone Number

- Physical Address

This data is collected in order to be able to ensure that the individual be kept informed of the progress of his order, and to have their purchases physically delivered. We store the data permanently. The reason for doing so is to have a record of the orders and who made them. This data will potentially be passed to wholesale suppliers. This is because a lot of products are directly shipped from wholesale distribution centres to the end customer.

Without collecting the End Customers name and address, the Client business would not know where to deliver the purchases to.

Without collecting the email address and telephone number, it would not be possible to deliver the products via direct shipment, as this is often a mandatory requirement by 3rd party couriers used by wholesale suppliers.

GDPR rights for individuals

Right to be forgotten

Stock Channel Ltd respects the wishes of individuals to have their personal details that have been legitimately collected to be deleted, and thus '*be forgotten*' by the organisation.

Stock Channel Ltd have created a mechanism that will delete all personal information regarding an individual from our records.

Procedure to request to '*be forgotten*'

The procedure for removing personal information for an individual is as follows;

1. Stock Channel Ltd receive a request from an individual or a person authorised by that individual to have their personal data removed. Requests will only be considered if received by physical post to Stock Channel's registered address, or electronically via a Stock Channel Ltd monitored email account. Should an individual make a right to be forgotten request by telephone or other electronic means, they will be asked to confirm their request by post or email.
2. The existence of an individual's record is appropriately confirmed.
3. Upon validation that this is a genuine request by the Data Protection Officer, an approval email will be sent to the designated IT Manager at Stock Channel Ltd.
4. The IT Manager will execute the mechanism described below to remove the individual's details.
5. The removal of the individual's details is validated by the Data Protection Officer
6. The individual requesting the right to be forgotten will then be notified by Data Protection Officer using the same communications method as the request was received by.

Measurable outcome of being forgotten

Upon receiving an approved, valid request to remove an individual's personal data, Stock Channel Ltd IT Manager will execute specially written software code which performs the following tasks;

1. Title, first and last name are overwritten with hashes (#)
2. Email is overwritten with hashes (#)
3. Telephone is overwritten with hashes (#)
4. All address details are overwritten with hashes (#)
5. Job title is overwritten with hashes (#)

Allowing users to edit their profile personal information

Upon Login, all Stock Channel Ltd Client business users have access to a personalised account page where they can maintain and update any of the personal details stored about them.

Data Portability – Subject Access Request

Stock Channel Ltd have created a mechanism that will provide visibility of all personal information collected about an individual, to that individual.

Procedure to submit a Subject Access Request

The procedure for requesting a copy of personal information collected about an individual is as follows;

1. Stock Channel Ltd receive a request from an individual or a person authorised by that individual to view a copy of their personal data. Requests will only be considered if received by physical post to Stock Channel's registered address, or electronically via a Stock Channel Ltd monitored email account. Should an individual make a Data Portability request by telephone or other electronic means, they will be asked to confirm their request by post or email.
2. The existence of an individual's record is appropriately confirmed.
3. Upon validation that this is a genuine request by the Data Protection Officer, an approval email will be sent to the designated IT Manager at Stock Channel Ltd.
4. IT Manager will execute the mechanism described below to create a file containing a copy of the personal details collected about the individual.
5. The file is sent to the requesting individual using the same communications method as the request was received by.

Measurable outcome of a subject access request

Upon receiving an approved, valid request to provide a copy of an individual's collected personal data, Stock Channel Ltd IT Manager will execute specially written software code. This code creates a Comma Separated Value (CSV) file containing a copy of the individual's collected personal data. This file is deleted after it has been sent to the individual.

Personal Data Use & Storage

Staff responsibilities

Everyone who works for or with Stock Channel Ltd has responsibility for ensuring data is collected, processed and stored appropriately. Everyone that handles personal data must ensure that it works in line with this policy and data protection principles. However, some people have key areas of responsibility;

Staff with Key Responsibilities

The Board of Directors.

- The board of directors is ultimately responsible for ensuring that Stock Channel Ltd meets its legal obligations.

The Data Protection Officer, (Currently Paul Meyers).

- Keeps the board updated about data protection responsibilities, risks and issues.
- Reviews all data protection procedures and related policies, in line with an agreed schedule.
- Arranges data protection training and advice for the people covered by this policy.
- Answers data protection questions from staff and anyone else covered by this policy.
- Deals with requests from individuals to view the personal details Stock Channel Ltd holds about them (also called 'subject access requests').
- Checks and approves contracts or agreements with third parties that may handle Stock Channel Ltd confidential data.

The IT Manager, (Currently Artiom Chilaru).

- Ensures all systems, services and equipment used for storing data meet acceptable security standards.
- Performs regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluates third-party services the company is considering using to store or process data, for example: cloud computing services.

The Marketing Manager, (Currently Simon Darby).

- Approves any data protection statements attached to communications such as emails and letters.
- Addresses any data protection queries from journalists or media outlets like newspapers.
- Ensures marketing initiatives abide by data protection principles, working with other staff where necessary.

General guidelines for all staff

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, staff should request it from their line managers.
- Stock Channel Ltd will provide training to all staff to help them understand their responsibilities when handling data.
- Staff should keep all data secure, by taking sensible precautions and following these guidelines.
- Strong passwords must be used and should never be shared.
- Personal details should not be disclosed to unauthorised people, neither within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and securely disposed of.
- Staff should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

These guidelines describe how and where data should be safely stored. Staff questions about storing data safely should be directed to the IT Manager

When data is stored electronically, it must be protected from causal unauthorised access, malicious hacking attempts and accidental deletion.

- Data should be protected by strong passwords that are changed regularly and never shared between staff.

- All Data stored on any removable media for the purposes of disaster recovery, (for example; USB Drives, Tapes and DVD) is automatically encrypted. This media should be securely taken offsite and locked away when not being used.
- As policy, general staff DO NOT use, (nor have the option to use) removeable media for temporary file storage.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, and stored securely, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. General staff DO NOT use Laptops or Mobile devices to access, process or store Data.
- All workstations and related devices used to access data are encrypted, and additionally secured.
- All servers and computers containing data should be protected by approved security software and a firewall.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When data is stored on paper and printouts, it should be kept in a secure place where unauthorised people cannot see it, for example; not left on a printer.
- When not required, the paper and printouts should be kept in a locked drawer or filing cabinet.
- Paper and printouts should be shredded and disposed of securely when no longer required.

Data use

Stock Channel Ltd cannot provide any substantive value to its clients and their end customers unless it can collect and process Personal Details. If personal details are secured to the extent that they cannot be accessed, Stock Channel would cease to be a viable business.

However, it is when this collected personal data is accessed and processed that it is at the greatest risk of loss, corruption and theft. Staff should therefore take great care to protect confidential data.

- When working with personal details, staff should ensure the screens of their computers are always locked when unattended.
- Personal data should not be shared informally. Data must be encrypted before being transferred electronically. In particular, it should never be sent externally by unencrypted email. The IT manager can explain how to send data to authorised external contacts.
- Staff should not save copies of personal data to their own computers. Staff should always access and update the central server copy of any data.
- Personal data should never be transferred outside of the European Economic Area.

Data accuracy

The law requires Stock Channel Ltd to take reasonable steps to ensure data is kept accurate and up to date. Further, Stock Channel prides itself on our overall data accuracy. It is most important that individual personal data is accurate, and staff should place great emphasis on ensuring its continued precision.

It is the responsibility of all staff who work with data to take all reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data should be held in as few places as possible. Staff should not create unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, for example: by confirming a Client business user's details when they call.
- Stock Channel Ltd should make it easy for data subjects to update the information Stock Channel Ltd holds about them. For instance, via their account page on the Stock Channel Ltd website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.