How to set up a fashion brand online

6131109_2

How to set up a fashion brand online

This guide highlights some of the key issues you will need to consider when setting up a fashion brand online. It is designed to give you a flavour of the sorts of issues you need to think but individual businesses will have different issues.

If I sell my clothes to a country outside the UK, am I responsible under foreign laws?

If your site is set up to sell garments to citizens based in a country outside the UK, then you are likely to be responsible under that country's laws for the garments you sell. Generally, you would need to be targeting a particular market, such as the US market. This may involve you quoting prices of your garments in US dollars and, perhaps, also using the US sizes when describing the item of clothing or even US terminology such "pants" instead of "trousers".

Mere accessibility in another country is unlikely to mean that you are responsible under that country's laws. The key test is whether your website is actively soliciting and fulfilling orders to, for example, US citizens. In this scenario, you should be complying with US law.

The global dimension of the web is both an incredible opportunity but also presents new risks and challenges. If you are selling garments and related items outside your home jurisdiction, then you need to be aware that national laws differ considerably. You need to give thought to how you manage this. There are also issues concerning conflicting national laws. For example, it is possible that English law requires you to do one thing and US law another. Also, the clothing brand that you've been using in the UK may well conflict with another brand in the new country where you are now trading over the Internet.

What do you do? Rock and a hard place springs to mind as there is no easy answer or solution.

Luckily, there are measures that you can take to address this issue. Which approach works best for you will depend on the size of your business.

For the truly large multinational business, one solution is to have separate country specific websites which reflect the country you are targeting. www.easyjet.co.uk has approximately 15 different sites. For most businesses, this is not commercially viable.

The approach adopted for the majority of online businesses is to make it clear which countries your website is targeting. This reduces the risk of you being legally responsible in a country in which your website is merely accessible. Your site should state clearly what countries you will and will not sell to and this should be reflected in your backoffice systems. They must be capable of rejecting orders from individuals in excluded jurisdictions. The starting point should be to limit your markets to the countries you are comfortable trading within.

If you have a registered EU trade mark, you may be comfortable trading in the EU without fear of infringing someone else's trade mark in the US, for example. Your terms and conditions play an important part in managing this risk. Your terms should contain relevant information about your chosen markets. The terms should also provide for a fairly detailed complaints procedure. The idea being to stop people suing, or making complaints to trade bodies, in their national jurisdictions.

Do I need to comply with the Data Protection Act? If so, what does this involve?

In the UK, the Data Protection Act 1998 ("DPA") regulates the use of personal information. If you collect personal data through your website such as customer names, addresses and other contact details, then you need to comply with the DPA.

Generally, if you are selling garments online you will collect some form of personal information such as the individual's name and delivery address.

There are a number of aspects to complying with the DPA.

1 Notifying the ICO

You will need to register with the UK Information Commissioner (or "ICO"). This is called "notification". The notification needs to set out the details of the way you will use information. It is a criminal offence to process data without being included on the register maintained by the Commissioner.

2 Privacy policy

You need to use the personal information you collect in accordance with the eight principles of good information handling which are set out in the DPA. These principles can be onerous to comply with. An important aspect of compliance is to prepare a privacy policy which sets out how you use the customer data you collect through your site.

Having a poorly drafted privacy policy, or not having one at all, can be fatal to your ability to comply with the DPA. There is also a customer expectation that websites will have a privacy policy. This makes the site look professional.

3 Subject access requests

Individuals have certain rights under the DPA that must be respected. In particular, there is a right under the DPA to get a copy of the information held about them subject to certain exceptions. Individuals also have a right to prevent the use of their personal data for direct marketing purposes.

4 The General Data Protection Regulation ("GDPR")

The GDPR comes into force on 25 May 2018 and will replace the DPA. Many of the concepts and principles will be the same. The important changes are:

i. *No requirement to "Notify" with the ICO* – instead the onus is placed on keeping accurate records demonstrating your compliance with data protection law.

ii. *Data Protection Officer ("DPO")* – if you are a business which carries out large scale regular and systematic monitoring of individuals (such as behaviour tracking) you will need to appoint a DPO as the first point of contact, internally and externally, for data protection matters.

iii. *Higher consent thresholds* – you will need to be sure that the consent you obtain from customers is given in a clear affirmative form. Silence, pre-ticked boxes or inactivity will not constitute consent. This is especially important when consent is being obtained to use customer's details for the purposes of direct marketing. Consent must also be able to be easily withdrawn by the customer.

iv. *Privacy Notices* – The GDPR requires more information to be given to the customer about the processing of their data. You may need to include more information in your privacy notices. At the same time, privacy notices must be concise, transparent, intelligible and easily accessible. They should be written in clear and plain language. There are a number of innovative ways which the GDPR envisages privacy information can be delivered effectively to the customer such as, layering (with links to more detailed information), providing "just-in-time" information, using privacy dashboards, standardised icons, animations and even videos.

v. *Other individual rights* – in addition to the right to submit subject access requests, individuals will have rights to transfer personal data between businesses ("portability"), the erasure of their personal data (the "right to be forgotten"), the right to rectify inaccurate personal data and the right to object to direct marketing.

What is a "cancellation right" and how does it affect me?

Customers who purchase items of clothing or other related items through your website have a right to cancel an order and return the goods for any reason. To do this, the customer must inform the retailer within fourteen working days after the day following delivery of the goods.

This cancellation period may be extended where the retailer fails to provide certain information as required by the Consumer Contracts Regulations:

i. If the required information is provided within 12 months of the first day of the normal 14-day cancellation period, the customer will have a further 14 days from when it receives the required information to cancel the purchase.

ii. If the required information is not provided within 12 months of the first day of the normal 14-day cancellation period, the cancellation period is extended to 12 months from the last day of the normal cancellation period.

The rationale behind the cancellation right is to allow the customer the opportunity to try the clothes or accessories as one would be able to in a shop. However, there are particular issues with garments where the customer not only tries on the garment but wears it to the office party and then seeks to return it. Retailers are understandably concerned about reselling items which have been worn or which may raise issues about hygiene.

Bespoke items – an exception

There are some exceptions to the right to cancel which may assist fashion retailers such as where the garments are bespoke, made to the customer's specification. This exception will apply for example to made to measure suits, but will not apply simply where there has been a selection based on standard options, such as colour or size.

Goods which cannot be returned – another exception

Another possible exception to the right of cancellation is in respect of "*rapidly deteriorating goods*". This could apply where returning the goods is a physical impossibility (e.g. they have been eaten) or where they cannot be restored in the same physical state as they were supplied no matter how they are cared for. In the fashion world, the exception may apply to items such as latex or nylon clothing which could become distorted once worn.

The cancellation right is burdensome to comply with. However, retailers can offset some of the downside by putting in place an appropriate returns policy and terms and conditions to deal with the issues raised by the cancellation right. For example, customers are not obliged to return clothes in a saleable condition but are required to take reasonable care of the goods. This is something that should be reflected in the returns policy and terms and conditions.

Who owns your website and can it use content and images found on the web?

A website is usually made up of software, content and images. A person "owns" a website by owning the intellectual property ("IP") in this software, content and images. Where a retailer commissions a site to be developed by an independent contractor the retailer is likely to believe that, as it is paying for the development, it should own all components of the work done. However, the fact that the retailer has commissioned and paid for the work does not inevitably mean that the IP in it legally belongs to the retailer. It will only do so if the IP has been transferred to the retailer. This would need to be included in the web development agreement.

Whilst ownership may be desirable, it is not essential. In order to publish the site, the retailer must either own the IP or have a licence to use it. There are no formal requirements for a licence, but it is in both sides' interest to have clear terms set out in writing. You need to make sure that any licence you get allows you to use your website as you intend. For example, you should make sure that your licence is on a world-wide basis if you are intending to sell clothes internationally.

Generally, a web developer will not wish to give away software coding which he can reuse in other website developments; he would regard these as his stock in trade. On the other hand, he may be happy to transfer ownership in components which have been specifically designed for the retailer. This may be important to the retailer, particularly where this gives a distinct competitive advantage.

Usually, a website will comprise IP that you own, for example, IP in content that you upload to the site and IP (e.g. in software) owned by a third party such as the developer.

You may also want to use images and content that you have sourced from the web and elsewhere. Quite simply, if you do not have permission to use these images and content, you should not be displaying them on your website.

This is important where you are displaying brands and logos of designers and fashion labels. You need to make sure that you have permission to use and display the logo and brand from the brand owner. The same rules apply where you are displaying an image or a photo of a model or celebrity, perhaps because they are wearing your label or clothes. Even though an image or photo is freely available on the web does not necessarily give you the right to use it for your own purposes. If you are using materials, photos or images without permission, then the owner may be entitled to claim damages from you.

Who is responsible for user comments posted on my site?

You – the website owner are responsible for users who post defamatory statements or infringe a third party's intellectual property rights (e.g. a text quotation or photo). This is most likely to arise in the context of any blogs and, potentially, your social media accounts. If you plan in advance, you may be entitled to a statutory defence.

In relation to libellous statements, websites may have the benefit of the "intermediaries' defence" or the "website operators' defence" under the Defamation Act 2013.

Whether the "intermediaries' defence" defence is available will depend on a number of factors such as whether the operator is considered editor or publisher of the statement, took reasonable care in relation to the publication and had no knowledge or reason to believe that its operations contributed to the publication of a defamatory statement.

The "website operators' defence" depends on whether the person who posted the statement is able to be "identified", and whether the claimant gave the operator notice of the complaint which the operator failed to respond to within the correct timeframes.

In relation to IP infringement claims, the websites operator may have a defence under copyright laws. Both of these specific defences are quite narrow and may be difficult to apply in practice.

What About Linking?

The Ecommerce Regulations contain more general defences that are designed to protect website operators. Under these regulations websites have a defence for hosting unlawful content where they:

1. do not have actual knowledge of the unlawful information;

2. are not aware of facts and circumstances from which it would have been apparent to a service provider that the information was unlawful; or

3. upon obtaining such knowledge, act quickly in removing it.

Again, this defence is not easy to apply in practice and leads to various questions. For IP infringement claims, whether the website has a profit-making intention will also be taken into account when determining whether the defence is available.

Should the website moderate content?

If content is moderated before being published and unlawful content slips through, then the operator will potentially be seen as a publisher or editor of that content and could be liable for it. There are also issues of censorship and freedom of expression which could be seen to be contrary to the user's expectation.

Depending on the system of moderation, this could also be a considerable logistical undertaking.

What about notice and takedown?

If websites do not moderate content, they need to put in place effective notice and take down procedures. This approach is not without risk either.

First, the website has to make an assessment as to whether content is unlawful. If this assessment is wrong and content is not taken down, then the defence will be lost and the website could be liable for the content. Similarly, if the website is overzealous in removing content, then it could be open to allegations of censorship and having an adverse effect on the user experience.

In addition, the availability of an operator to claim the "website operators' defence" is dependent on compliance with Defamation Regulations 2013 which include strict timeframes within which the operator must respond to a complainant. These will need to be incorporated into website operator's notice and takedown procedures.

Operating an effective notice and takedown procedure therefore requires clear polices to be put in place. These should be prepared carefully and will need to interact appropriately with your terms and conditions and the way in which the website is designed.

Are there any other laws I need to be aware of when selling online?

Fashion retailers trading online face a complex array of legislation with which to comply and face dealing with a number of UK and EU regulators that are keen to protect online shoppers.

The main laws you should be aware of are as follows.

Consumer Rights Act 2015 ("CRA")

The CRA, concerns two types of terms in standard terms and conditions: (i) terms which are limitations; and (ii) terms which are subject to a test of "fairness". The CRA applies to all kinds of standard terms of business that are used with consumers including website terms of sale.

Limitations which are never effective against a consumer include: limitations or exclusions of liability for death or personal injury caused by "negligence", exclusions in respect of the transfer of title of goods, exclusions of statutory implied terms relating to the characteristics of goods (these are correspondence with description or sample, satisfactory quality and fit for purpose).

An "unfair" term is not binding on the consumer which means a business can lose the protections it has included within the consumer contract. A term is "unfair" if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations under the contract to the detriment of the consumer.

The CRA also requires that contract terms are written in plain, intelligible language. If there is doubt about the meaning of a written term, the interpretation which is most favourable to the consumer is preferred.

Intelligibility depends not just on vocabulary but also on how contracts are presented. The online contracting process needs to be carefully designed to ensure that terms are presented fairly and are brought to the consumers' attention.

The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 ("CCR")

Online consumer sales are "distance contracts" which fall under the CCR. Compliance with the CCR requires that consumers be given certain information about the clothes or other goods on offer and the contractual process for purchasing such items.

Under the CCR, consumers also have a cancellation right exercisable during a limited period where they can reject the items they have purchased via the web for any reason (which is discussed in more detail above).

Compliance with the CCR should be engineered into the website and back-office development.

The CCR are designed to protect the consumers and can be burdensome for the retailer. This can be offset to some extent in terms and conditions of business.

The Electronic Commerce (EC Directive) Regulations 2002

The Ecommerce Regulations require you to include certain information about your business and your online contractual process on your website. This is usually provided in your website terms and conditions. The Ecommerce Regulations also contain rules concerning the form of unsolicited email communications with your customers and may provide you with a defence from legal actions arising from displaying illegal content (which is discussed in more detail above). This is important where you are allowing your users to post content and comments.

Privacy and Electronic Communications Regulations 2003

The Privacy Regulations establish rules for the sending of electronic marketing communications such as emails and texts.

Essentially, unless you have an "*existing business relationship*" with a person, then you must have a person's explicit consent before sending them any form of electronic marketing communication. You can obtain consent through the appropriate use of tick boxes on your website. The Privacy Regulations also require you to tell users if you use "cookies" and how a user may disable the use of cookies. This is something that is usually covered in your privacy policy.