Student Number: 220202684
Word Count: 3548

Technology: House of Maina
Collection and Processing of data transfer between the UK and a Third Country: Relevant Issues and Legal Compliance

Background:

House of Maina being a leading fashion enterprise that operates across two jurisdictions, must stay compliant to laws and guidelines in both, India and the United Kingdom. Entering a new market in the fashion industry would require extensive research into market viability, ongoing fashion trends, operability, legal compliance to name a few tasks that are necessary to prepare for the possibility of successful operations outside a label's home turf. The vision of House of Maina, i.e. to become a globally recognised beachwear brand embracing Indian beauty and craftsmanship comes with a challenge. However, with the right support, these tasks can be made less daunting to deal with.

Once market research has been completed, a strategy must be put into place, which House of Maina has very carefully devised to ensure successful operations in India and the United Kingdom. However, as House of Maina operates in the United Kingdom via its website and social media platforms with no stores brings with its own advantages and disadvantages. Using this model, House of Maina requires no permanent employees in the United Kingdom, and can rely on contractual arrangements for logistical and professional support. However, this would mean the brand would require a robust logistical network they can rely on in order to satisfy customer orders in a country with no employees on the ground. Further, because the brand is based in India and operates through its website, there are legal requirements to be met while collecting customer information which is capable of identifying an individual and includes information such as names, addresses, gender, email addresses, phone numbers, etc. These requirements include the protection of the information collected, prevention of misuse of such information, and deletion of such information, should it be requested by an individual that previously consented to providing information to the brand.

The brand's strategy in the United Kingdom includes collaborations with influencers to generate and sustain brand awareness, participation in fashion shows, high street pop-up events and consumer contests to reach a broader section of their target audience and newsletters at regular intervals to keep existing customers updated on new arrivals and brand news. In order to engage in these activities, the brand would require to collect personal information from potential customers as well. The collection of any and all personal information by the brand, would attract the provisions of the General Data Protection

Regulation.[1] While the Regulation applies to EU member states, the Data Protection Act 2018 is the implementation of the GDPR in the United Kingdom and must be read together.[2] In order to provide appropriate legal advice to the brand, this document will first deal with the existing laws surrounding data protection in the United Kingdom and move towards requirements to be met to operate within the bounds of the law.

The current law:

The General Data Protection Regulation is a comprehensive set of regulations that is set out to streamline data handling, privacy, storage and sharing of data across EU member states. It seek to provide enhanced layers of protection of personal information shared digitally and has been regarded as one of the strongest set of data protection regulations in the world. [3] Prior to the enforcement of the GDPR, member states were given time to adopt small changes in order to better suit the state's needs and in the United Kingdom, this lead to the Data Protection Act 2018. Further, the GDPR is a part of retained law from the EU post Brexit, and are to be read alongside the Data Protection Act.

The Data Protection Act 2018 was adopted in line with GDPR. The main focus of the law is the protection of personal data. Every individual, on a daily basis provides personal information to a number of service providers which may or may not be able to identify them. This brings up a number of privacy concerns in case of a data breach, or if the data is collected for one purpose but used for another, to name two.

There are seven fundamental principles that form the basis of the Data Protection Act and UK GDPR and form Article 5 of the UK GDPR. These principles are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.[4] Any and all data collection, processing and transfers are to be made on the basis of the seven fundamental principles. If not done in such a manner, the activity is deemed unlawful, and would attract severe penalties under the GDPR regime. These may include a fine up to £17.5 million or 4% of annual turnover, whichever is higher.[5]

---

[1] Regulation (EU) 2016/679, Article 5, General Data Protection Regulation (2016) of the European Parliament and of the Council, < https://www.legislation.gov.uk/eur/2016/679/contents> (last accessed on Aug. 23, 2023);
[2] Local Government Association, The General Data Protection Regulation (GDPR) Guidance for members, (2018) <https://www.local.gov.uk/sites/default/files/documents/The%2BGeneral%2BProtection%2BData%2BRegulation%2B%28GDPR%29%2B-%2BGuidance%2Bfor%2BMembers.pdf> (last accessed on Aug. 21, 2023);
[3] Matt Burgess, What is GDPR? The summary guide to GDPR compliance in the UK, Wired (2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018; ,
[4] Regulation (EU) 2016/679, Article 5, General Data Protection Regulation (2016) of the European Parliament and of the Council, < https://www.legislation.gov.uk/eur/2016/679/article/5 >; (last accessed on Aug. 22, 2023);
[5] The Information Commissioner's Office, A guide to the data protection principles https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/ ; (last accessed on Aug. 22, 2023);

Under the UK GDPR, a controller is defined as an individual/organisation/authority that exercises control over the entire process of data collection and processing.[6] They exercise control over processors as well. A processor is defined as an individual/organisation/authority which processes the data collected on behalf of the controller.[7]

Under the scheme of the UK GDPR, controllers and processors who are based outside the United Kingdom are subject to the regulations if the processing activities they undertake relate to either offering goods or services to individuals in the United Kingdom or are monitoring the behaviour of individuals taking place in the United Kingdom. Going by this, the UK GDPR is very much applicable to House of Maina as the brand offers goods to individuals residing in the United Kingdom. Data transfers that occur to controllers outside the United Kingdom are termed as 'restricted transfers'.[8] Restricted transfers are transfers containing personal data, hence, a transfer of data without personal information is not called a restricted transfer. Under the scheme of the UK GDPR, a restricted transfer is allowed to be made if the controller/receiver is located in a third country covered by something called 'adequacy regulations' which forms Article 45 of the UK GDPR.[9] Adequacy regulations are regulations that state that the legal framework in the third country has been assessed and provides adequate protection for the rights and freedoms for people's personal data.[10][11] Unfortunately, India is not a part of the adequacy regulations and we must move to Article 46, which provides for transfers that cannot take place as per adequacy regulations and are subject to appropriate safeguards.[12][13] Now, under Article 46, House of Maina would have to have standard data protection clauses that are specified in regulations by the Secretary of State.[14][15] However, there is another method of collecting personal data that the brand may employ. Under Article 49, exception 1 allows for the collection of personal data if "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy

---

[6] Regulation (EU) 2016/679, Article 4(7), General Data Protection Regulation (2016) of the European Parliament and of the Council, https://www.legislation.gov.uk/eur/2016/679/article/4 ; (last accessed on Aug. 19, 2023);
[7] Regulation (EU) 2016/679, Article 4(8), General Data Protection Regulation (2016) of the European Parliament and of the Council, https://www.legislation.gov.uk/eur/2016/679/article/4 ; (last accessed on Aug. 19, 2023);
[8] The Information Commissioner's Office, A guide to international transfers, last updated July 13, 2023 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/#rules ; (last accessed on Aug. 19, 2023);
[9] Regulation (EU) 2016/679, Article 45, General Data Protection Regulation (2016) of the European Parliament and of the Council,< https://www.legislation.gov.uk/eur/2016/679/article/45>(last accessed on Aug. 19, 2023);
[10] Supra note 8
[11] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74)
[12] Regulation (EU) 2016/679, Article 46, General Data Protection Regulation (2016) of the European Parliament and of the Council,< https://www.legislation.gov.uk/eur/2016/679/article/46 >(last accessed on Aug. 19, 2023);
[13] European Union Agency for Fundamental Rights/Council of Europe, Handbook on European Data Protection Law, 2018 Edition (2018);
[14] IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition (2020);
[15] SCCs and CoCs and BCR - Untangling the web and spotting the difference, International Network of Privacy Law Professionals (2021);

decision and appropriate safeguards;".[16] If the brand wishes to move forward under Article 49, they would have to provide a disclaimer providing information with respect to the collector of data, the location, possible risks involved due to the absence of adequacy decision and safeguards. However, it is possible that existing and/or potential customers might choose to not provide personal information if they understand the risks involved with transferring data to the brand's servers in India.

Further, pursuant to Section 4 Article 37 of the UK GDPR, House of Maina would require a data protection officer since it regularly processes data of individuals in the UK and must be an individual who has expert knowledge of data protection law and must fulfil tasks as per the UK GDPR. The data protection officer need not necessarily be an employee of the brand, they can fulfil their duties on a contractual basis as well, which negates the requirement to have employees in the UK that the brand may have to look after. Apart from a data protection officer, House of Maina would be required to appoint in writing a representative in the United Kingdom. The representative would be in addition or instead of the brand to be addressed by the Commissioner and individuals whose data is being collected on any and all issues related to data processing to ensure compliance with the UK GDPR.[17]

Recommended method of conducting business for House of Maina:

a. **Online sales:**

House of Maina intends to enter the UK market with the use of their website, high street pop ups and collaborations with local influencers to gain a customer base. The brand does not intend to open a physical store now or in the near future. With high street pop ups, the brand wishes to engage with women aged 18-35, collect their personal information for periodical newsletters, and convert them into customers. This strategy of the brand would require the collection and processing of personal data of individuals residing in the UK. This would mean that even though the brand is not a UK entity, the UK GDPR applies as it is providing goods/services to individuals residing in the UK.[18] The data collected would include names, addresses, phone numbers, email addresses, gender, ethnic origin and other similar information that are identifiable.

Under the UK GDPR, House of Maina is defined as a controller as they exercise control over information processing activities as well as collection of said information. The duty of compliance with the regulation lies with the controller, and

[16] Regulation (EU) 2016/679, Article 49, General Data Protection Regulation (2016) of the European Parliament and of the Council,<https://www.legislation.gov.uk/eur/2016/679/article/49>(last accessed on Aug. 21, 2023);
[17] Regulation (EU) 2016/679, Article 27, General Data Protection Regulation (2016) of the European Parliament and of the Council,<https://www.legislation.gov.uk/eur/2016/679/article/27>(last accessed on Aug. 21, 2023);
[18] The Information Commissioner's Office, The UK GDPR < https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/> (last accessed on Aug. 21, 2023);

thus, the brand must ensure compliance with the regulation in order for its information collection activities to be deemed lawful.

As a controller, House of Maina has the responsibility to appoint a representative in the UK that can be addressed with or instead of the brand who will be in charge of communication with the Information Commissioner and individuals whose data is being collected and processed by the controller and ensure compliance with the regulations. The role essentially comprises of liaising with the Information Commissioner and data subjects. The representative may either be an individual or a legal person that is capable of representing the controller appropriately.[19] Additionally, the representative has the duty to maintain a record of processing activities up to date and accurate to ensure compliance with the regulation.

Further, the controller has the duty to appoint a data protection officer as it collects and processes data frequently. The officer must be an expert in data protection law and allied laws, and must ensure compliance with the regulations as well. It is necessary to understand that the representative of the controller and data protection officer are two separate roles, and one individual cannot fulfil the duties of both, even though it may sound like the roles have some overlap. The controller cannot instruct a data protection officer who must be given the autonomy and independence to perform their duties.[20] The representative of the controller must act on the instructions and mandate provided by the controller and therefore, both roles cannot be exercised by the same individual or legal person.

It is the controller's duty to ensure the contact information for both, the data protection officer as well as the representative to be made available to all individuals from whom personal information is being collected for processing by the controller.

Moving ahead, a data transfer containing personal information to a third country i.e. outside the EEA and United Kingdom is called a restricted transfer. A restricted transfer contains information that is capable of being identified with a particular individual and must be protected with the utmost safety. Under the regulations, there are a number of ways and circumstances under which a restricted transfer may take place. They are:

1. Adequacy decision: an adequacy decision is a decision in law where the Secretary of State has been satisfied that the third country has adequate safety measures for

[19]European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), (2019) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf > (last accessed on Aug. 21, 2023);
[20] Article 29 Data Protection Working Party, 16/EN, <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100 >(last accessed on Aug. 21, 2023);

data protection. If the transfer is made as per an adequacy decision, there need not be specific authorisation for the same.[2122]

However, it is unfortunate that India does not fall under the adequacy decision. Hence, we move to the next point.

2. Transfers subject to appropriate safeguards: This applies in the absence of adequacy regulations. Under this article, a restricted transfer may be made to a third country only when the controller has provided safeguards and ensures that legal remedies are available to the data subjects.[23] These safeguards include standard data protection clauses specified in regulations made by the Secretary of State under the Data Protection Act 2018.[24]

3. Derogations for specific situations: Under Article 49, a restricted transfer can take place in the absence of an adequacy decision or appropriate safeguards if:

    i. There is explicit consent from the data subject for the transfer and consent has been obtained after informing the data subject of the possible risks of such a transfer without appropriate safeguards;[25]
    ii. The transfer is necessary or the performance of a contract between the data subject and controller or for the implementation of pre-contractual measures at the data subject's behest;

It is recommended that House of Maina undertake collection and processing of personal data of existing/potential customers while employing appropriate safeguards to protect their rights and information as per Article 46. Alongside harbouring under Article 46, House of Maina may obtain personal information from data subjects by obtaining explicit consent after informing the data subjects of the risks that might have been involved, but due to the use of standard data protection clauses, need not worry about their personal data not being appropriately protected.

Subsequently, House of Maina must maintain a record of processing activities which is the duty of the representative appointed by the brand under Article 27 of the UK GDPR. This record must be accurate and updated regularly.

b. Customer competition:

[21] Regulation (EU) 2016/679, Article 45, General Data Protection Regulation (2016) of the European Parliament and of the Council, <https://www.legislation.gov.uk/eur/2016/679/article/45>(last accessed on Aug. 22, 2023);
[22] Supra 11
[23] C. Kuner, L. Bygrave, and C. Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Article 46 GDPR, Oxford University Press (2020);
[24] Regulation (EU) 2016/679, Article 46, General Data Protection Regulation (2016) of the European Parliament and of the Council,< https://www.legislation.gov.uk/eur/2016/679/article/46 >(last accessed on Aug. 22, 2023);
[25] Supra 20

House of Maina intends to host a customer competition to increase brand awareness and engagement. The “Summer Style Getaway Contest” invites participants located in India and the United Kingdom and will be open for a period of one month. The participants must be aged 16 or above and submit an entry. The entry is a photo of the individual wearing House of Maina apparel, tag the brand in the photo on Instagram and must use the hashtag #VacaywithMaina. This information is gathered and collected as entries to the competition for entrants to be considered on criteria such as originality and creativity. The winner of the competition would win brand apparel.

The winning entry will be used by the brand for promotional activities, and hence the brand requires permission from the entrant to do so. There are underlying intellectual property considerations that are required to be deliberated upon as well which will not be dealt with here.

House of Maina must explicitly communicate the method of collection of participant data, how it will be stored, processed and used prior to entry into the competition. This information must be openly displayed so that participants understand what their information will be used for and the risks involved.

As mentioned above, the brand must either under Article 46, put in place appropriate safeguards such as standard data protection clauses, or under the first or second exception under Article 49 collect data with explicit consent or in order to fulfil the contract of the competition respectively. A recommendation is that appropriate safeguards are employed alongside obtaining explicit informed consent of the participants of the competition.

c. Newsletters:

In order to engage and educate existing customers and potential customers regarding the brand’s offering, House of Maina intends on sending periodical newsletters with curated content showcase origins of the brand’s design, style inspiration, sustainability initiatives, fashion tips, etc. Customers will have the option to subscribe to this periodical newsletter. To do so, customers would have to provide consent to the brand to use their personal information for the additional purpose of receiving the newsletter, which they previously may not have consented to. It is required by the brand to provide a full disclosure on what information they would be using for the purpose of sending existing/potential customers newsletters, provide the option of opting out if they wish to, and how such personal information would be stored.

Conclusion:

Upon reading the advice provided above, House of Maina will have a clear understanding of their obligations under the UK GDPR as a controller of data. Despite House of Maina being a non-UK entity, it is subject to the UK GDPR as it provides goods to individuals residing within the United Kingdom and must therefore aim to become and remain legally compliant with data protection regulations that exist in a market, they aim to be successful in. Non-compliance with the UK GDPR will undoubtedly result in humongous fines that may even be more than projected revenues from the new market and would also result in loss of trust with their customers and poor brand image.[26]

Currently, India does not fall under the adequacy decision under Article 45 of the UK GDPR. However, it is imperative to note that the Indian legislature has passed the Digital Personal Data Protection Act on 11th August 2023. The aim of the Act is "*An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto*"[27].

Under the UK Data Protection Act 2018, Section 17B states that the Secretary of State must continuously review and monitor developments in third countries that may affect decisions relating to adequacy decisions which could mean that the legal regime may change and House of Maina might be able to collect personal data without the requirement of standard data protection clauses under Article 46. However, currently, there is no shift in such a direction as it is a new law and it remains to be seen how it is implemented and how it is viewed by the Secretary of State. Therefore, House of Maina must comply by Article 46 and Article 49 of the UK GDPR along with other provisions mentioned above in order to stay above board and conduct its data collection in a legal manner.

[26] Paul Lambert, Complying with the Data Protection Regime, 2 International Journal for the Data Protection Officer, Privacy Officer & Privacy Counsel. 17 (2018);
[27] The Digital Personal Data Protection Act, 2023, Ministry of Law and Justice, Government of India, 2023 < https://egazette.gov.in/WriteReadData/2023/248045.pdf > (last accessed on Aug. 22, 2023);