

Privacy Impact Assessment

Name:- Gaurav Sood
Student ID:- s5372043
Course Code:- 7905ICT

Name:- Akash Muraleedharan Nair
Student ID:- s5386260
Course Code:- 7905ICT

Name:- Aryan Hari
Student ID:- s5394883
Course Code:-7905ICT

Executive Summary

The purpose of this Privacy Impact Assessment is to find possible breaches of 13 APP as defined in Australian Privacy Principles. This assessment involves how the user data is being taken from HelloFresh how HelloFresh protects the user data, how it is stored in the HelloFresh server and how Hellofresh discloses the user data to the third party and whether this disclose information about the user in accordance with the 13 Australian privacy principles. A privacy impact assessment is done to check how a company/project impacts the privacy of their users and sets out recommendations for managing, minimising and eliminating the impact. This report includes complete data flow/information flow for the HelloFresh and 13 privacy impact and compliance checks with the identification of the risks and recommendations that HelloFresh can use to resolve the impact and protect users personal information. (Oaic, 2023d),(Oaic, 2023c),(Oaic, 2023b),(Oaic, 2023a).

Description of the project

Background of Hellofresh:- <https://www.hellofresh.com.au/>

HelloFresh is a meal kit delivery service that sends weekly meals with fresh ingredients and a recipe card for a family of two or more. The business model of the company is the weekly meal kit which acts as an alternative for grocery shopping and meal planning. HelloFresh provides a pre-measured quantity of food for two or more people which prevents food waste. The cost for a meal kit is around 40-70 AUD which depends on the number of people and number of boxes an individual requires each week. (*HelloFresh: #1 Food Box Delivery Service | Healthy Meals*, n.d.)HelloFresh provides 25 fresh recipes every week with different categories from protein-rich meal boxes to calorie-smart boxes which makes it a perfect business model for any individual looking for healthy variations in their meals. (*High-Quality Meal Kits | Get up to \$150 Off!*, n.d.)

HelloFresh operates in the US, United Kingdom, Australia, New Zealand, Canada and many European countries.

HelloFresh meal kits are sustainable by nature, this means that the company directly takes raw materials from Australian supply and delivers the meal kit directly to the consumer removing all the detours of the traditional supply chain. Thus HelloFresh meal kits are 15% more sustainable than the ingredients found in the supermarket. (HelloFresh, 2022)

Information Flow

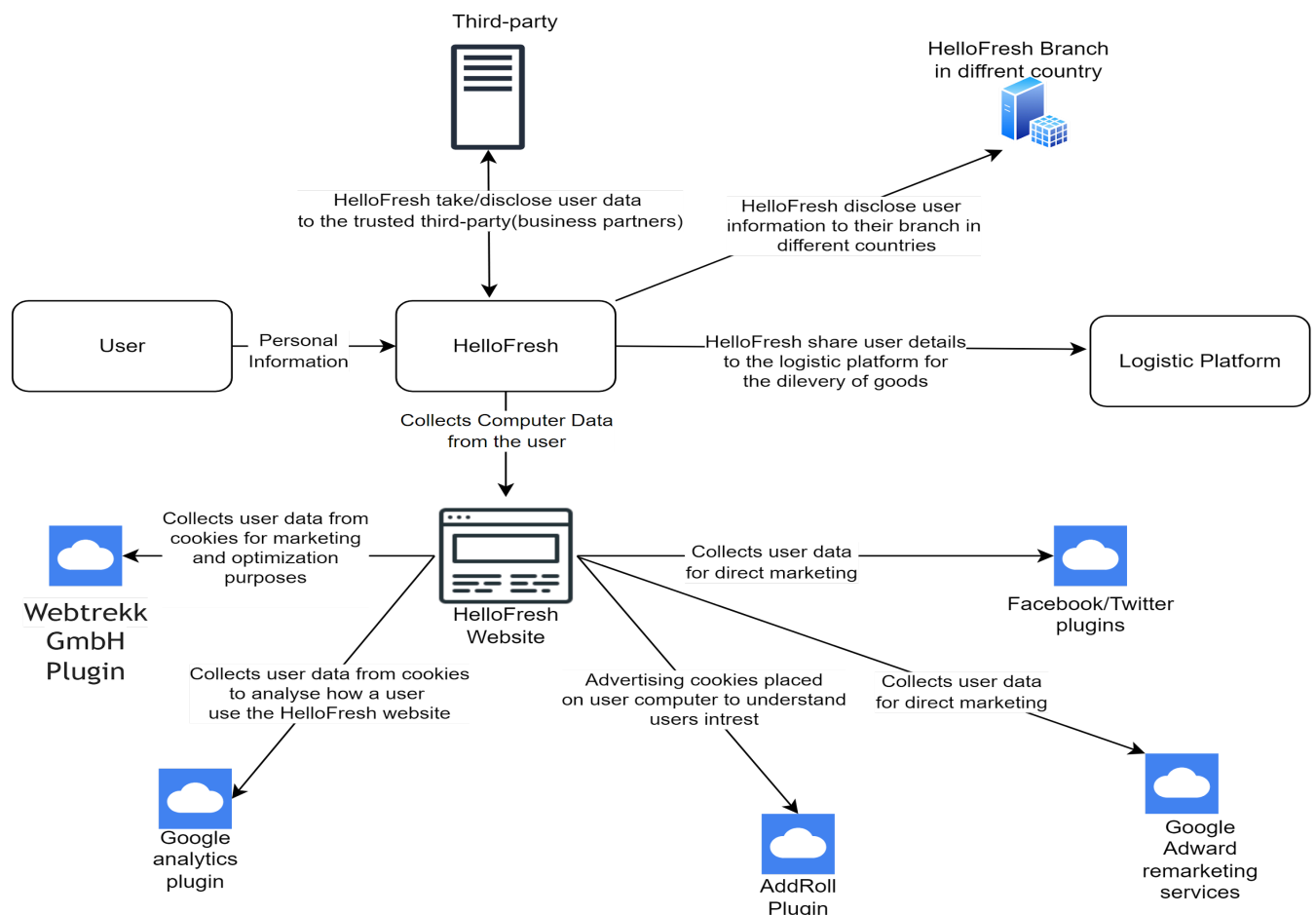


Fig:- Made using Draw.io

HelloFresh take personal information such as name, delivery address, email, contact number, age, gender and credit card information which are required to interact with the HelloFresh services. (*Privacy*, n.d.)

HelloFresh collects computer data such as device IP address, device type, browser type, device data and information about previous web pages before visiting the HelloFresh website. (*Privacy*, n.d.)

HelloFresh websites have embedded many plugins that have different purposes, such as

- Webtrekk Gmbh Plugins which collects data for marketing and optimization purposes. Here the data is stored in cookies and it gets saved temporarily at the local cache of the user browser. (*Privacy*, n.d.)
- Google Analytics plugins collect user data that are stored in cookies, and text files saved on the users hard drive which helps google to analyze how a user uses the HelloFresh website. The information gathered by the user cookies is transmitted to Google servers in the US and saved there. (*Privacy*, n.d.)
- HelloFresh website places advertising cookies on users computers to understand user interests and also helps with direct marketing. (*Privacy*, n.d.)
- HelloFresh website has embedded plugins for Facebook and Twitter which form a direct connection from the company website to these social platforms. These social platform collects the data from cookies as a user surfs through the website and uses this information for direct marketing. (*Privacy*, n.d.)
- HelloFresh website also uses Google Adwords remarketing services to advertise on Google and third-party websites using user cookies. (*Privacy*, n.d.)

HelloFresh takes additional user information from a trusted third party that also holds some other information about the user. HelloFresh also discloses users personal information to a trusted third party. This trusted third party combines information to develop consumer insights such that HelloFresh can get a better understanding of the users preferences and interests. (*Privacy*, n.d.)

HelloFresh also discloses information to other HelloFresh groups which are located within and outside Australia, including Europe, North America and Oceania. (*Privacy*, n.d.)

HelloFresh provides limited user details to the logistics partner for the delivery of the weekly meal kits. (*Privacy*, n.d.)

Privacy Analysis and Compliance Check

References are taken from the following:-

(Privacy, n.d.)

(Griffith University & Tian, n.d.-a)

(Griffith University & Tian, n.d.-b)

(Oaic, 2023a)

(Oaic, 2023b)

(Oaic, 2023c)

(Oaic, 2023d)

(Undertaking a Privacy Impact Assessment — a Free eLearning Course From the Office of the Australian Information Commissioner, n.d.)

| Privacy Principles | Implemented information handling practices | Identified risks/Comments |
|---|--|---|
| APP1 - Open and transparent management of personal information <ul style="list-style-type: none">• An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code and is able to deal with related inquiries and complaints.• An APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.• An APP entity must take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website).• An APP entity must, upon request, take reasonable steps to provide a person or | <p>HelloFresh collects personal information from users or from their trusted third party.</p> <p>HelloFresh uses this information to deliver the product, user eligibility for the service and optimise user experience.</p> <p>Hello Fresh explains in their policy How they collect and why they collect personal information</p> <p>HelloFresh Ensures transparency between users (Privacy, n.d.)</p> | <p>Hello Fresh follows with APP1 and ensures that it is open and transparent about taking personal information from the user.</p> <p>HelloFresh mentions they can change their policy with time and it will be updated on</p> |

| | | |
|--|---|--|
| body with a copy of its APP Privacy Policy in the particular form requested. | | their website accordingly |
| <p>APP 2 — Anonymity and pseudonymity</p> <ul style="list-style-type: none"> An APP entity is not required to provide those options where: <ul style="list-style-type: none"> the entity is required or authorised by law or a court or tribunal order to deal with identified individuals, or it is impracticable for the entity to deal with individuals who have not identified themselves Anonymity means that an individual dealing with an APP entity cannot be identified and the entity does not collect personal information or identifiers. A pseudonym is a name, term or descriptor that is different to an individual's actual name. Where applicable, an APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity. | <p>HelloFresh collects personal information from the users directly by taking information from the user or from a trusted third party.</p> <p>HelloFresh does not provide means for the user to be Anonymous or use</p> <p>HelloFresh did not clearly mention whether full anonymity is possible when using their service.</p> <p>A user can use a pseudonym name but it has not been made aware to the user by HelloFresh in their privacy policy.(Privacy, n.d.)</p> | <p>HelloFresh does not follow APP2 which leads to privacy concerns if a user wants to be anonymous and interact anonymously with the services.</p> |
| <p>APP 3 — Collection of solicited personal information</p> <ul style="list-style-type: none"> An APP entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information. For personal information (other than sensitive information), an APP entity that is: <ul style="list-style-type: none"> an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities Personal information must only be collected by lawful and fair means. | <p>HelloFresh takes user personal information like: name, phone number, delivery address, mailing address, credit card information and other information that users provide while visiting the HelloFresh website.</p> <p>HelloFresh needs these details from the user to let the easy use of their service for the user.</p> <p>HelloFresh mentions in their policy why they collect these data, how they will use the data and how they are going to disclose users personal information to the third party.(Privacy, n.d.)</p> | <p>HelloFresh follows APP3 and it collects personal information from the user and lawful and fair means.</p> <p>If HelloFresh had collected data without the user consent it would be against APP3</p> |

| | | |
|--|---|--|
| <p>APP4 --- Dealing with unsolicited personal information</p> <p>An APP entity that receives unsolicited personal information must decide whether or not it could have collected the information under APP 3, and:</p> <ul style="list-style-type: none"> • if the entity could not have collected the personal information and the information is not contained in a Commonwealth record — the entity must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so, or • if the entity could have collected the personal information under APP 3, or the information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the information because it would be unlawful or unreasonable to do so — the entity may keep the information but must deal with it in accordance with APPs 5–13. | <p>HelloFresh collects information about the user from a trusted third party.</p> <p>HelloFresh receives personal information about the user from their trusted third party. These third parties might have additional information about the user which might not be required by HelloFresh for its primary purpose.</p> <p>If HelloFresh receives additional information, they have not mentioned in their privacy policy whether the additional information should be destroyed or de-identified (<i>Privacy</i>, n.d.)</p> | <p>Hello Fresh does not follow APP4 which can cause privacy concerns for the user.</p> <p>HelloFresh should determine whether the information can be collected by the APP3 and if not they should either destroy/de-identify the information or the information should be in compliance with APP5-13.</p> <p>Collection of unsolicited information can lead to data mishandling within the organization and also privacy breaches for the users.</p> |
| <p>APP 5 — Notification of the collection of personal information</p> <ul style="list-style-type: none"> • An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. • The matters include: <ul style="list-style-type: none"> o the APP entity's identity and contact details o the fact and circumstances of collection o whether the collection is required or authorised by law o the purposes of collection | <p>HelloFresh in their privacy policy states that it notifies users when they collect their personal information, what they collect the information and who might share this information.</p> <p>(<i>Privacy</i>, n.d.)</p> <p>HelloFresh collects users' data from the plugins embedded in their website such as Google Analytics, Facebook and Twitter.</p> <p>HelloFresh mentions in its privacy policy about the</p> | <p>HelloFresh partially follows APP5 and ensures to make the user aware of the collection of personal information.</p> <p>If Hellofresh notified users every time they collect data from the embedded plugins and get consent from</p> |

| | | |
|--|---|---|
| <ul style="list-style-type: none"> o the consequences if personal information is not collected o the entity's usual disclosures of personal information of the kind collected by the entity o information about the entity's APP Privacy Policy o whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located | <p>collections but it has not been directly made aware to the user nor notification is sent to the users when collecting these data(<i>Privacy</i>, n.d.)</p> | <p>the user then it would have followed APP5 completely.</p> |
| <p>APP 6 — Use or disclosure of personal information</p> <ul style="list-style-type: none"> • An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. • The exceptions include where: <ul style="list-style-type: none"> o the individual has consented to a secondary use or disclosure o the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose o the secondary use or disclosure is required or authorized by or under an Australian law or a court/tribunal order o a permitted general situation exists in relation to the secondary use or disclosure o the APP entity is an organization and a permitted health situation exists in relation to the secondary use or disclosure o the APP entity reasonably believes that the secondary use or disclosure is | <p>Hellofresh disclose user information to the trusted third party who also holds information about the user .</p> <p>HelloFresh does not de-identify the user information before giving it to the third party, also as mentioned in the privacy policy the third party also holds some information about the user. Thus the third party can trace back to the individual user therefore breaching the privacy policy of APP6.</p> <p>HelloFresh disclose user information to third parties which they use to develop anonymized consumer insights for a better understanding of consumer preference. This is a breach of APP6 as it is done for a secondary purpose.</p> <p>HelloFresh can only disclose personal information for the purpose it was collected.</p> <p>If HelloFresh wants to get consumer insight for better understanding then they must de-identify the user information before</p> | <p>HelloFresh does not follow APP6.</p> <p>De-identifying the user information is important for the compliance of the APP6, as it will allow the App entity to disclose information for secondary purposes to the third party without breaching APP6.</p> |

| | | |
|--|---|---|
| <p>reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or</p> <ul style="list-style-type: none"> o the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 | <p>disclosing it to the third party.(Privacy, n.d.)</p> | |
| <p>APP 7 — direct marketing</p> <p>An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented.</p> <p>Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:</p> <ul style="list-style-type: none"> • allow an individual to request not to receive direct marketing communications (also known as ‘opting out’), and • comply with that request. <p>An organisation must provide its source for an individual’s personal information, if requested to do so by the individual.</p> | <p>HelloFresh uses personal information to send direct marketing to individual users with an option to opt out.</p> <p>HelloFresh places advertising cookies as a user browses through the website to know their interest. The websites display partner AdRoll based on the user’s previous interaction. Hellofresh provides users with an option to opt out of the AdRoll.</p> <p>HelloFresh uses a service called Webtrekk GmbH to collect and store data for marketing purposes. The data is used to create a user profile anonymously. The collected data is then deleted when no longer needed. HelloFresh provides an option to opt out.</p> <p>HelloFresh also uses GoogleAdWord remarketing, Facebook and Twitter plugins with an option to opt-out by logging out of Facebook/Twitter before</p> | <p>Hellofresh partially follows APP 7 and it ensures a simple way for a user to opt out of direct marketing communications .</p> <p>If HelloFresh provided a mechanism on its website for opting out of direct marketing through Facebook/Twitter rather than logging out of the respective websites before surfing Hellofresh then it would have followed APP7 completely.</p> |

| | | |
|---|---|--|
| | using the HelloFresh website.(Privacy, n.d.) | |
| <p>APP 8 — cross-border disclosure of personal information</p> <p>Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.</p> <p>An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act).</p> | <p>HelloFresh provides information to its staff, group members, holding company, and subsidiaries located both inside and outside of Australia, including in North America, Europe, and Oceania. HelloFresh has not stated in its privacy policy that it will make sure the other foreign company abides by the app regulations put in place by the Australian government.</p> <p>The privacy policy does not clearly state that HelloFresh will bear liability for any personal information provided to foreign recipients or third parties.</p> <p>HelloFresh websites use Google Analytics that transmits information by cookies when a user surfs through the HelloFresh website and this gathered information is stored in the US servers, here HelloFresh does not ensure that Google provides privacy protection in accordance with the 1-13 APP.(Privacy, n.d.)</p> | <p>HelloFresh does not follow APP8.</p> <p>Personal data transfers to nations with less strict privacy regulations increase the possibility of abuse, security breaches, and restricted individual recourse.</p> |
| <p>APP 9 — Adoption, use or disclosure of government related identifiers</p> <ul style="list-style-type: none"> An identifier is a number, letter or symbol, or a combination of any or all those things, that is used to identify the individual or to verify the identity of the individual. A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a | <p>HelloFresh generally obeys the law as they don't take any government-related identifier as their own identifier for an individual.</p> <p>Hello Fresh does not ask for any government-related identity for the verification instead it has its own identity verification. They verify a user contact</p> | <p>HelloFresh compliance with APP9</p> <p>As the law is being followed, it minimizes the risk of third-party access towards the government identity which</p> |

| | | |
|---|---|--|
| <p>contracted service provider for a Commonwealth or State contract.</p> <ul style="list-style-type: none"> Where an identifier, including a government related identifier, is personal information, it must be handled in accordance with the APPs. An organisation must not adopt a government related identifier of an individual as its own identifier of the individual, unless an exception applies. An organization must not use or disclose a government related identifier of an individual, unless an exception applies. | <p>number/email by sending an OTP.</p> <p>(<i>Privacy</i>, n.d.)</p> | <p>results in the exposure of personal information.</p> <p>If a government ID was used to identify a user in HelloFresh then any third party with whom HelloFresh share data can easily trace back to the individual user</p> |
| <p>APP 10 — Quality of personal information</p> <ul style="list-style-type: none"> An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. | <p>HelloFresh maintains the Quality of personal information by verifying the details of a user.</p> <p>HelloFresh verifies users by sending them OTP on their email/contact number.</p> <p>HelloFresh also provides a mechanism for the user to update/correct their details if the data gets inaccurate by visiting</p> <p>https://www.hellofresh.com.au/account-settings/account-info/edit-personal-info</p> <p>Alternatively users can also contact customer care(<i>Privacy</i>, n.d.)</p> | <p>HelloFresh compliance with APP 10 .</p> <p>If APP 10 was not followed by HelloFresh then it would have led to incorrect data, which could cause a risk, such as outdated/ inaccurate information</p> <p>Inaccurate information including name, phone number, and address, resulting in miscommunication and inaccuracies in product deliveries.</p> |
| <ul style="list-style-type: none"> APP 11 — Security of personal information An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. | <p>HelloFresh ensures that all information collected will be safely and securely stored by restricting access to personal information, and maintaining technology products to prevent</p> | <p>HelloFresh partially follows APP 11 and it should provide some security measures by ensuring that</p> |

| | | |
|--|---|--|
| <ul style="list-style-type: none"> Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. This requirement applies except where: <ul style="list-style-type: none"> the personal information is part of a Commonwealth record, or the APP entity is required by law or a court/tribunal order to retain the personal information | <p>unauthorized computer access. Securely destroying users' personal information when it's no longer needed for retention purposes.</p> <p>Hellofresh uses 128-bitSSL encryption technology method when processing users' financial details.</p> <p>HelloFresh integrates its website with plugins from the social network Facebook and social service Twitter. These plugins form direct contact from the browser to the social sites, transmitting the data to these sites(<i>Privacy</i>, n.d.)</p> | <p>these social sites are according to the privacy policy</p> |
| <ul style="list-style-type: none"> APP 12 — Access to personal information APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request. APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access. APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to information, including, for agencies, the Freedom of Information Act 1982 (FOI Act) that provides a right of access to information held by agencies. | <p>HelloFresh complies with APP 12; according to their privacy policy, users have the right to access the user data that HelloFresh keeps about them, as well as the right to request that personal information be updated. If the user's personal information is incorrect or out of date, they can update it at any time by logging into their account.</p> <p>HelloFresh also protects our personal information by restricting unauthorised access</p> <p>According to the HelloFresh policy, In exceptional circumstances, HelloFresh may be required to disclose personal information, such as when there are grounds to believe that the disclosure is necessary to prevent a threat to life or health, or for law enforcement purposes. Moreover, the user has the right to ask HelloFresh not</p> | <p>HelloFresh Compliance with APP12</p> <p>Users have the right to access their information and the right to update their details.</p> |

| | | |
|--|---|---|
| | to disclose their personal information to other parties. (<i>Privacy</i> , n.d.) | |
| <p>APP 13 — Correction of personal information</p> <ul style="list-style-type: none"> • APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. • This requirement applies where: <ul style="list-style-type: none"> o the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or o the individual requests the entity to correct the personal information. | <p>HelloFresh provides the right to request access for the users to their personal information held by them. HelloFresh also provides a link to update their personal information anytime if they find it outdated or inaccurate by accessing their user account.</p> <p>HelloFresh also provides help through their customer service team to help their users.(<i>Privacy</i>, n.d.)</p> | <p>HelloFresh provides a mechanism to help the user correct their personal information through their website.</p> <p>If HelloFresh does not follow then, the information of the users given to the third party gets updated by them. This may lead to the risk of misinformation.</p> |

Addressing risks and Recommendations

References are taken from the following:-

(Privacy, n.d.)

(Griffith University & Tian, n.d.-a)

(Griffith University & Tian, n.d.-b)

(Oaic, 2023a)

(Oaic, 2023b)

(Oaic, 2023c)

(Oaic, 2023d)

(Undertaking a Privacy Impact Assessment — a Free eLearning Course From the Office of the Australian Information Commissioner, n.d.)

| # | Identified privacy risk | Existing controls that contribute to managing the identified risk | Recommended actions | Comments |
|---|--|---|--|----------|
| 1 | HelloFresh does not allow users to be anonymous or made aware that users could use pseudonym names | <ul style="list-style-type: none">-HelloFresh collects information directly from the user or trusted third party which holds information about the user-HelloFresh did not mention in their privacy policy whether a user could interact with their services anonymously-A user can input a pseudonym name but it has not been made aware by the Hellofresh (Privacy, n.d.) | <ul style="list-style-type: none">-HelloFresh should make a portal where user can just provide their email, credit card and address for the delivery of goods-HelloFresh should state in their policy about using the pseudonym name.-If a user uses a pseudonym name, Hellofresh should verify user by sending an OTP to user email/contact number to prevent any scams | |
| 2 | Tracing back to the user with received information/misuse | -HelloFresh mentions in its policy they collect additional information | -HelloFresh should destroy/ de-identify any additional | |

| | | | | |
|---|---|--|--|--|
| | with the user personal information | <p>from a trusted third party.</p> <p>-This additional information may have a government-related identifier which could be used to trace back an individual user. This additional information could also be misused thus breaching the user privacy.</p> <p>(Privacy, n.d.)</p> | <p>information that does not satisfy their primary purposes.</p> <p>- Any information used for secondary purposes should either be destroyed or de-identify</p> | |
| 3 | Not making the user aware of the data being collected using plugins | <p>-Google Analytics, Facebook, Twitter and other plugins embedded in the HelloFresh websites collect user information using user browsing history and cookies.</p> <p>(Privacy, n.d.)</p> | <p>-HelloFresh should send a notification/ask for consent from the user before letting these plugins take data from the user's cookies.</p> <p>- HelloFresh should provide a portal where a user could opt-out of all the plugins through one click rather than opting out of each individually.</p> | |
| 4 | Not de-identifying users record before disclosing it to the third party | <p>-Hellofresh discloses users information to a third party to gain anonymous insight about the user interests.</p> <p>-Hellofresh did not mention in their privacy policy whether they de-identify the records before disclosing them.</p> <p>-HelloFresh can only disclose the information that is required for primary purposes and if the information is being disclosed for secondary purposes it should get de-identified</p> <p>(Privacy, n.d.)</p> | <p>- HelloFresh should de-identify the users record before giving it to the third party.</p> <p>-De-identifying the user record is important as it will help to protect users privacy and there would be no misuse of the consumer information.</p> | |

| | | | | |
|---|--|--|---|--|
| 5 | Opting out of direct marketing by Facebook | <p>-HelloFresh website is embedded with a Facebook plugin that collects user data for direct marketing</p> <p>-When a user surfs through the HelloFresh website the plugins form a direct connection to Facebook and the only way to opt out is to log out of Facebook before surfing through Hellofresh.</p> <p>(Privacy, n.d.)</p> | -HelloFresh should provide a mechanism to opt-out of Facebook direct marketing, instead of logging out of Facebook. | |
| 6 | Cross Border disclose of information | <p>-HelloFresh disclose the user data to its other branches outside of Australia</p> <p>-GoogleAnalytics which is embedded inside of the Hellofresh website saves users data at its US server to analyze user insights.</p> <p>-Hellofresh does not guarantee that data is transmitted across borders in compliance with APP 2-13</p> <p>(Privacy, n.d.)</p> | -HelloFresh should make sure that the data which is being transmitted follows APP 2-13 | |
| 7 | Security of users personal information | <p>-HelloFresh integrates its website with Facebook and Twitter plugins which collect data for direct marketing purposes</p> <p>(Privacy, n.d.)</p> | -Hellofresh should provide security measures so that these social platforms comply with the Australian Privacy Policy | |

Conclusion and Reflections

HelloFresh should comply with the 13 APP and not doing so would be a breach of consumer privacy. HelloFresh should update its privacy policy and implement a mechanism for anonymity, de-identifying users records, providing one portal to opt-out from all direct marketing communications and improving security for handling users personal information.

HelloFresh should have regular audits to maintain the trust of consumers and protect their privacy.

According to the Privacy Impact Assessment Hellofresh needs to improve their privacy policy and provide more details on how they handle user information briefly.

Hellofresh should always ensure transparency between users and should always take user consent before collecting/disclosing user personal information.

HelloFresh can strengthen its privacy by implementing the recommendations outlined in the privacy impact assessment and can achieve customer trust.

Contributions:-

Name:- Gaurav Sood
Student ID:- s5372043
Course Code:- 7905ICT
Contribution:- 34%

Name:- Akash Muraleedharan Nair
Student ID:- s5386260
Course Code:- 7905ICT
Contribution:- 33%

Name:- Aryan Hari
Student ID:- s5394883
Course Code:-7905ICT
Contribution:- 33%

References

HelloFresh. (n.d.). *Contact HelloFresh Australia: Customer Support and Enquiries*.

HelloFresh. <https://www.hellofresh.com.au/about>

HelloFresh. (2022). *Sustainability at HelloFresh*. HelloFresh.

<https://www.hellofresh.com.au/about/sustainability>

HelloFresh: #1 Food Box Delivery Service | Healthy Meals. (n.d.). Www.hellofresh.com.au.

<https://www.hellofresh.com.au>

High-quality meal kits | Get up to \$150 off! (n.d.). HelloFresh.

<https://www.hellofresh.com.au/meal-kits>

Griffith University, & Tian, H. (n.d.-a). *Fundamentals of cyber security*.

Griffith University, & Tian, H. (n.d.-b). *Privacy Impact Assessment Security Operations
Outline Assignment*.

HelloFresh. (n.d.). *Privacy | HelloFresh*. HelloFresh.

<https://www.hellofresh.com.au/about/privacy>

Privacy Impact Assessment. (n.d.). In *7905ICT Assignment* (p. 1 of 8).

*Undertaking a Privacy Impact Assessment — a free eLearning course from the Office of the
Australian Information Commissioner*. (n.d.). Office of the Australian Information
Commissioner. <https://education.oaic.gov.au/elearning/pia/topic5.html>

Oaic. (2023, October 25). *Guide to undertaking privacy impact assessments*. OAIC.

[https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-
agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessmen
ts#s6-privacy-impact-analysis-and-compliance-check](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments#s6-privacy-impact-analysis-and-compliance-check)

Oaic. (2023a, October 18). *The Privacy Act*. OAIC.

<https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act>

Oaic. (2023c, October 25). *Guide to undertaking privacy impact assessments*. OAIC.

<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments#s6-privacy-impact-analysis-and-compliance-check>

Oaic. (2023a, October 9). *Australian Privacy Principles quick reference*. OAIC.

<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference>