This Privacy Notice gives you an overview of the processing of your personal data in the context of the use of the offers and online Services on our Website and the corresponding App (hereinafter referred to as the "Service").
Furthermore, this Privacy Notice informs you about your rights and the possibilities you have to control your personal data and to protect your privacy.
We have always taken the protection of your personal data very seriously and - as before - will continue to take Appropriate organisational, contractual and technical measures to protect your data from unauthorised or unlawful processing and against accidental loss, destruction or damage.

1. Details of the Controller

The data controller is Ideawise Limited, Room 604, Alliance Building, 133 Connaught Road, Central Hong Kong, Hong Kong. Its representative is SmH ServiceCenter.de GmbH, P.O.

Box: 20 04 34, 13514 Berlin, Tel. 0800/3335521 (free of charge*), Fax. 0049 30-338405-999 (local charges Apply), please direct any general support requests to: support@fuck.com).

Ideawise Limited is also meant when the terms "we" or "us" are used below. Please note that we are a company based outside the European Economic Area ("EEA"). As far as you use our Service and data is processed, these data are transferred to a so-called "third country". Details can be found in section 7 below. You can contact our data protection officer at: datenschutz@fuck.com.(general support request will not be processed by the data protection team, please direct these request to support@fuck.com).

*Different rates Apply for calls from mobile phones.

2. Information on the Types of Data Processed and Their Origin

If we provide the Service for your use, we process personal data from various sources. This is data that we collect automatically - for example when you visit a Website - as well as other data that you have additionally provided to us.

a. Types of Data That We Automatically Collect

When you visit our Website, you submit technical information to our servers. This hAppens regardless of whether you subsequently register with an account with us to use the Service or not. In any case, the following data will be processed:

- During every visit of our Website:

The so-called server log. This is a file which stores the following data: the time, the status of your Website visit (status means in this case whether the visit of the Website was successful or not) as well as the request that your browser has made to the server to open the page, the amount of data transferred and the Website from which you came to the requested page (referrer), and the product and version information of the browser used (user agent).

- When you open the App:

If you create a profile on our Service, we will assign a so-called unique user ID to it. Besides your chosen profile name, the unchangeable Unique User ID allows us to uniquely assign your profile.

We also use cookies and API tokens to process this data. Cookies are small text files that you download to your device and that store the above information about you when you use our Services. API tokens are unique identifier files that we use for authentication when you request access to our Service. If you want to learn more about how cookies and API tokens

work, what cookies and API tokens we use, and where you can find opt-out options, click here.

b. Types of Data You Transmit to Us

In addition to the data we receive from all Website visitors, we also process other data from registered users.

The exact amount of this data depends on how you use the Service.

Personal information that you publicly upload to your profile or other areas of the Service will be visible to other users (and searchable via the search function within the Service). If you choose additional settings for the publication of your data, this information will also be accessible to users who are not logged in. The privacy settings can be determined by you in your profile settings.

The data you provide us with include:

i. User account / profile data:

To use the Service, you can create a user account (a "Profile"). When you create a Profile, you must provide some mandatory information to complete the registration.
Required is:
- Username
- Password
- Email address
- Gender
- Country
- City and postcode
- Date of birth
- What gender is searched for
- What you are looking for (one-night stand, affair...)

If you have uploaded an image, other users have the option of sending the image directly from our Service to Google Image Search using the "Classify Images" function. This way, other users can help us to better recognize fake profiles and unauthorized uploaded images. Of course this does not Apply where you have uploaded an image to your secret gallery.

ii. Optional Profile Information:

The use of the Service is possible only with the aforementioned information. However, you may also provide additional personal information in your Profile, such as physical characteristics, personal interests or detailed information about your sexual preferences, political opinion or ideological beliefs. If you want to, you can upload your personal photos

and videos to your Profile or a secret gallery. The scope of this optional data can be determined by you via the respective input fields in your Profile settings.

iii. Location Data:

When you register with our Service, we use your IP once to determine your Approximate location data. You can agree to this localisation when registering or change it if necessary.

iv. Communication Data: Users

If you communicate with other users of our Service, we save your conversation history so that the conversation history with your chat partners can be permanently displayed and conduct checks on certain keywords indicating criminal activity.

v. Communication Data: Customer Service

When you contact our Customer Service, written communications between you and the Service staff and notes on each transaction are stored so that you can always have a smooth customer Service experience when the transaction is resumed by other Service staff.

vi. Data for Age Verification and Fake Detection:

To perform the age verification (FSK18 check), we need a video from you. You must be in the video. In addition, your date of birth must be clearly visible on an official identity card. This way, we can verify that you are in fact of age.

Alternatively you can do the age verification also in connection with a Schufa information.

If you are suspected to be a fake, you must have your profile verified. To do this, you need to upload an image that shows your face. You must also visibly hold a note in your hand stating your user name and the current date.

vii. Social Sign-On:

You can also use the "Login with Facebook" function to create your profile. If you choose this function, you send us your username on the social network at www.facebook.com ("Facebook"), your email address with which you registered on Facebook, as well as your gender, first name and your profile picture.

3. Processing Purposes & Legal Bases

We process your data exclusively for the following defined purposes:

- to allow you and other users to use the Service and to ensure its functionality
- to provide you with additional Services that you have purchased
- to keep you up to date with relevant information about our Service and to send you system notifications to the e-mail address you have provided.
- to adapt the provision of the Service to your needs
- to display advertising tailored to your interests (including participation in prize competitions, discount campaigns, user surveys for market research and sweepstakes)
- to continuously improve the Service offer and to correct errors
- to detect and prevent fraud attempts
- to ensure the protection of minors
- to enable the exchange with customer Service in case of questions
- to check information published on your profile or shared by you through the Service
- to disclose your personal data to third parties if we are legally obliged to do so
- to assert legal claims and to defend against legal disputes
- to ensure IT security and operation of our systems
- to assist the competent authorities in discovering and prosecuting criminal offences including, but not limited to, offences causing bodily injury or death of the victims

In doing so, we rely on various legal bases in accordance with the so-called General Data Protection Regulation, a European Union legal framework for the standardisation of data protection law (“GDPR” for short). We refer in detail to the following legal bases:

Your consent (Art. 6 (1) lit. a GDPR)

When visiting the Website without registration, you agree to the cookie guidelines in the pop-up. If you have given us your consent to process personal data for specific purposes, this consent ensures the legality of the processing. By registering and creating your profile, you expressly agree to its use for the purposes described in detail in this Privacy Notice by ticking the box before sending off the registration form. So, if we process your data, it is because you have expressly allowed us to do so when you registered. Your consent is therefore the most important legal basis for the processing of your personal data by us. If you provide us with information about your sexual orientation or preferences, we will process this data exclusively on the basis of your consent.

Fulfilment of contractual obligations (Art. 6 (1) lit. b GDPR)

At the same time, the processing of personal data takes place also for the provision of the Service and in the context of the performance of our contract with you. In many cases, the processing is not only justified by your consent, but also because it is necessary to fulfil our contract with you: In order to fulfil your claim to the Services described in more detail in our General Terms and Conditions, it may be necessary, for example, to process your personal data. For example, if you wish to pay for your Vip or Premium membership the processing of your payment information is required for this.

Protecting vital interests (Art. 6 (1) lit. d GDPR)

We invoke this legal basis in narrowly defined case constellations (e.g. reported suicide announcements) where the processing is necessary for the protection of the vital interests of the data subject or another natural person.

Safeguarding legitimate interests (Art. 6 (1) lit. f GDPR)

By registering to use the Service, you consent to the processing of your data in accordance with this Privacy Notice. That is why we process your data in principle, because you have allowed us to do so. However, there are some cases in which we would be entitled to process your data without your consent because it is necessary to protect our legitimate interests (or the interests of third parties). In this respect, the purposes for which we process your data also represent legitimate interests. We pursue legitimate interests, for example, if we check images or texts for content relevant under Applicable criminal law or if we take measures to secure our “virtual domiciliary rights” as provider of the Service and in protection of other users. In these cases, we will not ask you in advance whether you agree to this processing, since processing is otherwise permitted by law.

Legal requirements or in the public interest (Art. 6 (1) lit. c & e GDPR)

In addition, we are legally obliged to provide certain information to criminal prosecution or tax authorities in individual cases upon request.

4. Data Sharing?

We treat your personal data with care and confidentiality and will only pass them on to third parties to the extent described below and not beyond.

a. To Other Users:

As our Service is a platform for getting to know each other, it is in the nature of things that we forward your profile data as well as other data (e.g. news you write and other communication you have with other users and the community) at your request and on your behalf to the corresponding users of the Service.

b. To Group Companies:

We transfer data to affiliated companies which form part of the same group of companies as us within the framework of strict protection requirements. This is the case, for example, when you make a customer service request. We will then forward this request to SmH ServiceCenter.de GmbH, a service company associated with us. In addition, our development company, TheNetCircle Network Co. Ltd. as well as the debt collection

partners Compay GmbH and Faircollect GmbH and the community management and marketing at Playamedia S.L. receive the necessary information to ensure the security and functionality of the Service and the handling of payments.

c. Third parties and Other Recipients (Both When Using Web and App):

In addition, we transmit data to external service providers who enable us to provide the Service to you. These include hosting providers, delivery service providers, payment service providers and providers of analytics platforms. We require each of these service providers to comply with strict rules about the security of your personal information when processing personal information on our behalf. Such processing operations are therefore based on contractual clauses guaranteeing an adequate level of protection for your data.

Affiliate Systems

We use the following affiliate systems to attract new customers to our community. We measure success on the basis of registrations and revenue.

Adcell: We use the Adcell partner program, a service of Firstlead GmbH (www.adcell.de). Tracking cookies are also set here. As soon as you click on an advertisement with the partner link, a cookie is set. In addition, the advertisements contain so-called tracking pixels. The information generated by cookies and tracking pixels about the use of this Website (including the IP address and delivery of advertising formats) is transmitted to a server of Firstlead GmbH and stored there. Among other things, Firstlead GmbH / ADCELL can recognize that the partner link on our Website has been clicked. This is how visitor traffic can be evaluated. These data are not merged with other stored data. Under https://www.adcell.de/datenschutz you can get more information about how the Adcell affiliate program processes data. If you wish to object to the processing of data within the framework of the Adcell partner program, you can do so here: <font color="#ffff00">-=https://www.adcell.de/transaction/notrack/active/0.=- sync:ßÇÈâÈâ

Google Adwords: We also use Google Adwords in conjunction with the Google Tag Manager to promote our site in Google search results and on third-party sites. Google uses a remarketing cookie that contains a pseudonymous cookie ID and information about the use of our Website. In this way, we can show you advertising that is in line with your interests. You can disable the cookie here: https://tools.google.com/dlpage/gaoptout?hl=en

Hasoffers/TUNE: We also use the Hasoffers partner program of the provider TUNE, Inc., which functions in the same way as the Adcell partner program. Further information can be found at <font color="#ffff00">-=https://www.hasoffers.com/privacy-policy/.=- proudly presents

Microsoft Bing Ads & Microsoft Conversion Tracking: This Website uses the tracking function of Microsoft Corporation (location USA, Privacy Shield certified), which is usually activated

automatically as soon as you access our Website via an ad placed by us via the online search platform Bing.com (hereinafter: "Bing Ads"). In this case, Bing Ads places a cookie on your computer, which enables us as a Bing Ads customer and Microsoft to recognize that you have visited our Website by clicking on a Bing Ads ad. The information obtained in this way about the total number of users who have reached our Website via a Bing Ad is used exclusively to generate conversion statistics and does not provide us with any personal information about the identity of the user. Your data will be processed in accordance with Art. 6 (1) lit. f GDPR. We do not store any personal data about you. We have no knowledge of the storage period at Microsoft and have no influence on it.

If you want to suspend the tracking process by Microsoft Bing Ads, you must avoid assigning cookies to your computer. Please activate the Appropriate opt-out function on the http://choice.microsoft.com/de-de/opt-out page. For more information about the cookies used by Microsoft Bing and Microsoft Inc.'s privacy policy, visit the Microsoft Bing Web site at http://privacy.microsoft.com/DE-DE/ to be taken from.

Amazon S3

This hosting service (processing in USA and Europe, Privacy Shield certified) is used by us to store and deliver videos and images.

Public Authorities

We transmit data to authorities in the event of a legal obligation based on a request for information from the respective authority.

BS Payone

In the shop it is possible to pay with PayPal. This is done via the payment provider BS Payone (location Germany, Appropriate level of data protection). When purchasing, we only transmit the user ID to BS Payone.

Compay

Our subsidiary (located in Germany, adequate level of data protection) is our debt collection partner. When purchasing a membership or points, the billing information is passed directly to Compay. Here you can see what data is involved.

The Shop

Our shop works together with a Dropshipper. This is PickPack Versand GmbH (location Germany, Appropriate data protection level). When you purchase an item, the billing information will include the order number, name, phone number, email address, company and address, if any, when you purchased the item. In addition, the product data (such as price, size, quantity and article number), the payment method and the shipping options.

Facebook

We use Facebook (location USA, Privacy Shield certified) for the function "Log in with Facebook". The data required for registration (e-mail address, date of birth, first name, profile photo) is transferred from Facebook to us.

Google

Google LLC is a Privacy Shield certified provider from the USA. Google Analytics is used to analyze the behavior of users of our services. With the help of Google Captcha, we can determine whether a visitor is a human being or a machine for certain actions. YouTube videos are embedded in our service in "advanced privacy mode". While no Youtube cookies are set due to this particularly data protection-friendly method of embedding, calling up the pages nevertheless leads to a connection being established with YouTube and the DoubleClick network. A click on the video can trigger further data processing operations over which we have no control.

Kayako

Kayako (UK location, adequate level of data protection) is our system for dealing with customer queries. With each request the e-mail address, your preview profile picture and the username will be transmitted.

onage

Our e-mail newsletters are sent via the technical service provider Ongage Ltd. (Location Israel, Appropriate level of data protection), to which we will send the e-mail address, nickname, registration date, gender, payment class, last login time, chosen language, "search by" gender, interests marked with "like", age, sexuality, newsletter unsubscribe info and bounce status, as well as the location stored in the profile. Ongage uses this information to send and statistically evaluate the newsletter on our behalf. For evaluation purposes, the e-mails sent also contain so-called web beacons or tracking pixels, which represent one-pixel image files invisible to the user. This allows us to determine whether a newsletter message has been opened and which links have been clicked. In addition, technical information is recorded (e.g. time of access, IP address, browser type and operating system). The data is collected exclusively under a pseudonym and is not linked to your other personal data, we cannot attribute this data to you as a person. These data are evaluated exclusively for statistical purposes. The results of these analyses can be used to better tailor future newsletters to the interests of recipients. In addition, Ongage may also use this data pursuant to Art. 6 (1) lit. f GDPR for its own legitimate interest in designing and optimising the service to meet its needs and for market research purposes, e.g. to determine the origin of the recipient countries. However, Ongage never uses the usage data of our newsletter recipients to identify recipients or to disclose the data to third parties.

If you wish to object to the data analysis for statistical evaluation purposes, you must unsubscribe from the newsletter by clicking the opt-out button at the end of each message or by submitting an e-mail objection to the processing. Because Ongage is a provider based in

Israel, your information will always be protected at an Appropriate level. Ongage's privacy policy can be viewed here: https://www.ongage.com/wp-content/data-privacy.pdf.

Paysafecard.com

Paysafecard.com (branch of the Prepaid Services Company Limited located in Germany, adequate level of data protection) is a payment provider for anonymous payments. With a Paysafecard you can buy a membership or points. If you select Paysafecard when you purchase, the User ID will be passed to Paysafecard.com and the email address will be passed to our own payment provider Compay.

Twilio

We use Twilio (location USA, Privacy Shield certified) for our free SMS service. If this function is used, the recipient's telephone number and the SMS text are transferred.

Typeform

With this survey program (location Spain, adequate level of data protection) we improve and maintain our community through a permanent feedback survey, as well as regular quizzes, other surveys and evaluations. Which information is passed on to Typeform depends on the respective survey, furthermore you decide yourself what you enter here. Among other things, the nickname, the sex, the payment class, information about the device (operating system, model, manufacturer and mobile phone provider) as well as the location stored in the profile can be transferred.

Vendo

Vendo (location Switzerland, adequate level of data protection) is an alternative payment provider for payments outside Germany, Austria and Switzerland. When purchasing a membership or points, the User ID will be forwarded directly to Vendo.

Virtual Business Support

In order to unlock uploaded pictures even faster, we work together with Virtual Business Support (Philippines). There new pictures are arranged by technical personnel. For the Philippines there is currently no adequacy decision of the European Commission, the processing is based on your explicit consent according to Art. 49 GDPR, and is based on data processing agreements and standard contract clauses.

d. Third parties (only when using the App):

Adjust

Adjust (location Germany, adequate level of data protection) we use for the usage evaluation and analysis of marketing activities. When you open the App, Adjust collects installation and event data. We use this information to understand how our users interact with our App and to analyze mobile ad campaigns. For such an analysis Adjust uses your anonymized IDFA

(iOS) or GAID (Android) as well as your anonymized IP address. It is not possible to identify you individually.

Apple

We use Apple (USA, Privacy Shield certified) and its Apple Push Notification Service (APNS) to send push notifications to iOS users that may contain personally identifiable information.

Facebook SDK

The Facebook SDK (USA, Privacy Shield certified) included in our App helps us to increase the success of Facebook advertising campaigns by, for example, not displaying ads on devices on which this App is already installed. In addition, the Facebook SDK allows for various evaluations of the installation of the App and of the success of the advertising campaign. In addition, individual activities (events) of the user within the App can be analyzed in order to better define the target group for advertising campaigns, for example. For this purpose, we send Facebook pseudonymous data, such as the time, model name of the device, IP address, name of the App, a unique Ad-ID created by Facebook, and the information that the App has been started. The Advertising ID provided by the operating system of the terminal device serves as the pseudonym. The latter occurs regardless of whether the user uses Facebook or not. Facebook uses this information to create a profile for the Ad-ID along with other information and uses this profile for promotional purposes.

Sentry

We work with "Sentry" from Functional Software, Inc. (USA, Privacy Shield certified) to detect and eliminate errors that occur in our backend. In the event of a crash or other unexpected error, information such as the version of the operating system and some technical data about the cause of the error is sent to Sentry. However, this information does not contain any personal data. We only use the data to increase the stability of our App.

More Google Services

Google Fabric (incl. Crashlytics and Answers) and Google Firebase (both: USA, Privacy Shield certified) help us to monitor the performance of our App, identify crashes and analyze user behavior. We use Google Firebase and its Firebase Cloud Messaging (FCM) service to send push notifications to Android and iOS users that may contain personally identifiable information.

Advertising Networks & Affiliates

When you use our App, our ad networks and affiliates may use so-called device identifiers to create an anonymous profile of your click behavior for mobile advertising. In our App we work with various mobile advertising partners, including the following companies (the link to the current privacy policy and an option to disable behavioral advertising, if available, can be found in our cookie matrix. Further information on the stored data can be obtained there):

- MoPub (location USA, Privacy-Shield certified)
- Liftoff (Location USA, Privacy-Shield certified)

- AppLovin (location USA, Privacy-Shield certified)
- Chartboost (Location USA, Privacy-Shield certified)
- Apple Search Ads (location USA, Privacy-Shield certified)
- Creative Matters (location Spain, adequate level of data protection)
- Fyber (location Germany, adequate level of data protection)
- Glispa (location Germany, adequate level of data protection)

These cookies and device identifiers can be used to display personalized advertisements to you. A profile is also created based on comparable information obtained by Google, Facebook, and other third-party ad networks (see list above) from your visits to other Websites or Apps on their networks.

Deactivation of personalized advertising in the App

You can disable personalized advertising by setting your device:

Android
Under Android, this option can be found in the Google Preferences App. Depending on the device, this is called "Google Settings" or only "Settings". Under the menu item "Google" -> "Ads" you will find the option "Deactivate Interest Based Advertising" or "Deactivate Personalized Advertising" depending on the device. The selection can be used to deactivate personalized advertising.

iOS
Under iOS this option is located in the App "Settings". Under the menu item "Privacy" -> "Advertising" you will find the option "No Ad Tracking". The selection can be used to deactivate personalized advertising.

5. Processing of Payment Ddata

When purchasing on our service through the Website or mobile Website, we transfer different information to our collection partners for each payment method. Our partners are Compay GmbH, Vendo Services GmbH, Paysafecard.com Services and BS PAYONE GmbH. Here you can find out which data this is for each desired payment method. If you want to use paid offers via the App, you will be provided with different additional information depending on the chosen payment method. However, you will not transfer this information to us, but will transfer it directly to the Apple App Store or the Google Play Store after you have given your consent to the terms and conditions and privacy policy. You make the purchases directly through the relevant store.

6. Information on Behavioural Advertising

“Behavioral advertising" means the use of tracking measures to determine the potential interest of users in advertisements on our Website and in our App and to display them in accordance with their interests. For this we use the following features: Gender, membership type, FSK-18 status, preferences, interest in membership, number of logins and which

gender a member is looking for. Members with a Premium and VIP membership have the possibility to turn off the advertising.

7. Transfer to Countries Outside the EU or the EEA

All servers of the Service are located in the European Economic Area ("EEA"), so your data do not technically leave the EEA for the time being, but the technical provision and processing of the data for the operation of the service takes place in the European Union.
However, when you submit information to us, it is legally transferred to a country outside the EEA because we are based in Hong Kong (P.R. China). In addition, our development company is also based in China, from where it has technical access to the servers in the European Union (EU).
According to the GDPR, China is a so-called "Third Country" in which no adequate level of data protection can be guaranteed in principle; there is no corresponding adequacy decision and no specific guarantees to compensate for this deficit. This means that, from a European perspective, personal data and data subjects there enjoy less protection and rights, as would be the case, for example, with processing operations in Australia, Russia or India.

If we transfer data to a third country, we generally guarantee an adequate level of data protection. This applies regardless of whether it is a transfer to an affiliated company or to another recipient (such as an external service provider). In these cases, we will ensure that the transfer is either based on approved standard contractual clauses, or that providers in the United States are certified under the EU-US Privacy Shield Program, or that there is another appropriate guarantee of an adequate level of data protection.

8. How Long Will my Data be Stored?

We process and store your personal data for as long as it is necessary for the fulfilment of our contractual or legal obligations. Thus, we store the data in principle only as long as our contractual relationship with you exists and also after termination only as far as the laws of the Federal Republic of Germany and the People's Republic of China require this. If the data are no longer necessary for the fulfilment of such obligations, they shall be deleted regularly and without delay, unless their further processing is necessary for the protection of legitimate interests or for the preservation of evidence within the framework of statutes of limitations. In this sense, in particular the storage of age verification and fake suspicion photos and videos is carried out expressly for the entire duration of the contract, since we hold this data in particular for the ongoing guarantee of the protection of minors and the prevention of fraud attempts.

The data collected under 2.a are stored for 180 days. This storage period serves our protection against attacks on the systems of our service, e.g. by so-called Distributed Denial of Service attacks, in which the systems are deliberately overloaded by a large number of accesses to our service in order to interrupt the provision of our service.

9. Information on the Voluntary Nature of the Information Provided

You are not legally obliged to provide us with the above data. In principle, the contractual relationship that you have entered into with us by agreeing to our General Terms and Conditions does not result in any obligation to provide this personal data. However, the transmission of the compulsory data is a basic requirement for a conclusion of a contract with us. In addition, if you do not provide us with certain information or if you object to its use, you may not be able to use the Service, or only to a limited extent. This is because the service essentially only becomes "alive" through the content posted by the users.

10. Information About Your Rights

You can assert the following rights:

Your right to information according to article 15 GDPR,
Your right to rectification according to article 16 GDPR,
Your right to erasure according to article 17 GDPR,
Your right to restriction of processing in accordance with Article 18 GDPR as well as
Your right to data portability under Article 20 GDPR.

If you have any questions in this regard, please contact customer service at support@fuck.com.

You can revoke your consent to the processing of personal data at any time.

In addition, you have the right to lodge a complaint with the responsible data protection supervisory authority.

11. Information About Your Right of Objection

a. Right of Objection in Individual Cases

In addition to the rights already mentioned, you have the right, for reasons arising from your particular situation, to object at any time to the processing of personal data relating to you on the basis of Article 6 (1) lit. f GDPR (data processing on the basis of a balancing of interests). If you object, we will no longer process your personal data unless we can prove compelling reasons for processing worthy of protection which outweigh your interests, rights and freedoms, or the processing serves the assertion, exercise or defence of legal claims.

b. Right to Object to the Processing of Data for Advertising Purposes

You also have the right to object at any time to the processing of your personal data for the purpose of direct marketing. If you object, we will no longer process your personal data.

Please also note the information in Section 9 of this Privacy Policy: If we terminate the processing due to your objection, it may be that the service can no longer be made available to you or only to a limited extent.
The objection can be made in each case form-free and should be addressed to support@fuck.com if possible.

12. Amendment of the Privacy Statement

We reserve the right to occasionally adapt parts of this Privacy Statement which do not require consent so that they always comply with the current legal requirements or to implement changes to our services in the Privacy Statement, e.g. when introducing new services. Your new visit will then be subject to the new privacy policy. If your prior consent is required for a change to our services or for the introduction of a new service, we will inform you in good time and ask for your consent.