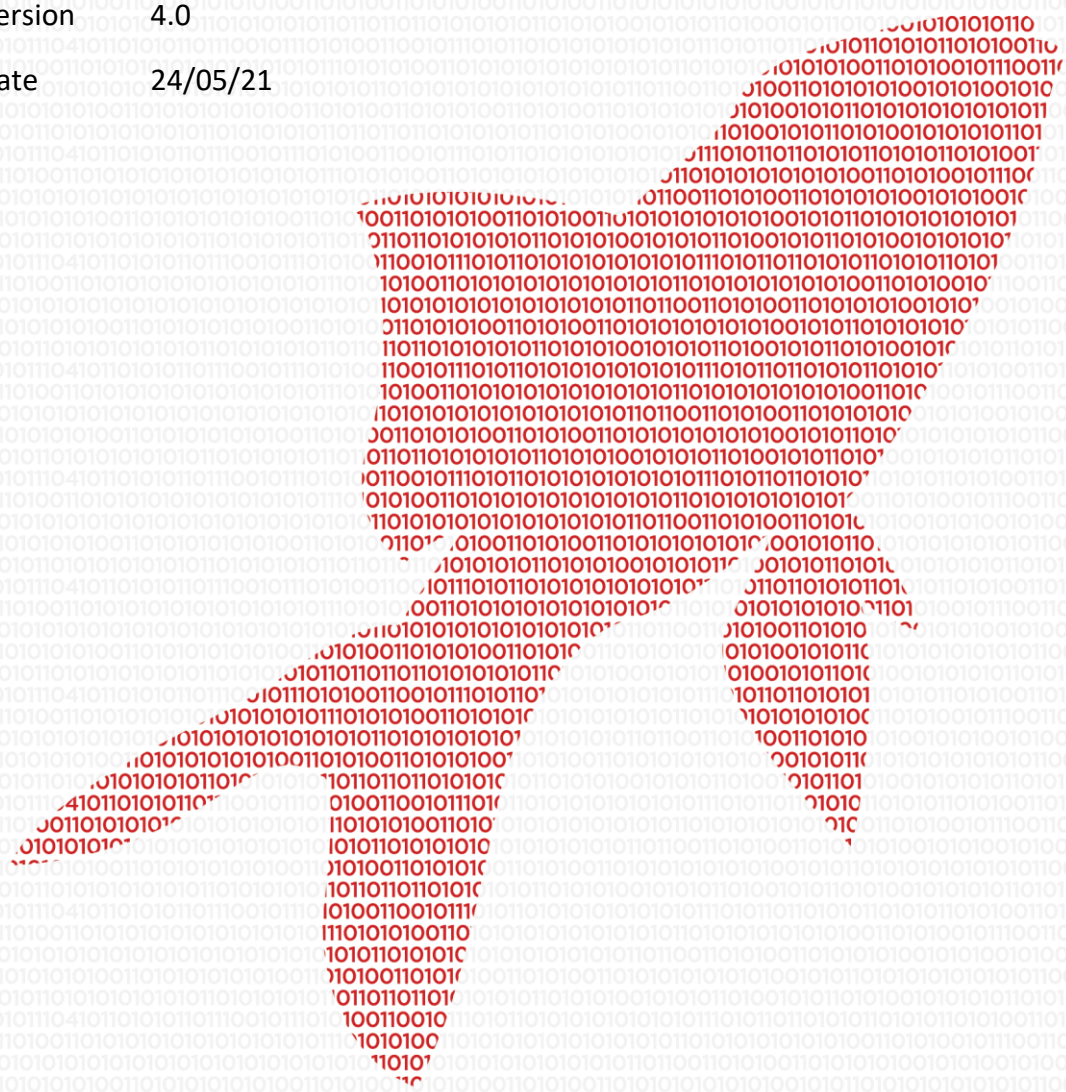
BLOCKPHISH

BLOCKPHISH Privacy Policy

Author	Tom Pepper
Version	4.0
Date	24/05/21



Contents

Document Information

Version	Date	Description	Author
0.1	22/05/2018	First Draft	Tom Pepper
0.2	23/05/2018	Updates following internal review	Tom Pepper
1.0	24/05/2018	Version 1.0 published	Tom Pepper
1.1	21/05/2019	Annual review	Tom Pepper
2.0	24/05/2019	Version 2.0 published	Tom Pepper
2.1	21/05/2020	Annual Review	Tom Pepper
3.0	24/05/2020	Version 3.0 published	Tom Pepper
3.1	21/05/2021	Annual Review	Tom Pepper
4.0	24/05/2021	Version 4.0 published	Tom Pepper

Authorisation Sign-off

Name	Organisation	Role	Date
Daryl Flack	BLOCKPHISH	CIO	**24/05/21**
Andy Green	BLOCKPHISH	CEO	**24/05/21**

1. Purpose

This privacy policy describes how BLOCKPHISH collects and uses personal information about you in accordance with the applicable data protection legislation.

BLOCKPHISH recognises the importance of this data and the risks related to its possession of such data. BLOCKPHISH is committed to protecting the privacy and security of your personal information.

BLOCKPHISH is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. To comply with data protection legislation and best practice we are required to notify you of the information contained in this privacy policy.

This policy sets out your rights under applicable data protection laws as well as our commitment to you regarding how we treat your data. We may update this policy at any time.

It is important that you read this policy, together with any other privacy policy we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

2. About BLOCKPHISH

BLOCKPHISH provides organisations with the ability to improve their resilience against phishing attacks. Our innovative features include:

- Bespoke ethical phishing campaigns mimicking current cyber threats
- Feedback to users who take the phishing bait
- Comprehensive reporting to track organisational progress
- Tailored awareness learning using a proven portfolio of methods and techniques

We have appointed a Data Protection Officer to oversee compliance with this privacy policy. If you have any questions about this privacy policy or how we handle your personal information, please contact the Data Protection Officer, contact details of whom are set out in Section 3.0. You have the right to make a complaint at any time for data protection and privacy issues.

3. Data Protection Officer

	Daryl Flack
	BLOCKPHISH Ltd.
	4th Floor, Silverstream House, 45 Fitzroy Street, Fitzrovia, London, W1T 6EB 0845 86 22 365
Regulator:	Information Commissioner's Office

4. Data Protection Principles

BLOCKPHISH has committed to applying the highest standards of data protection in accordance with applicable data protection regulations. This means that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

5. The Information We Hold About You

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, store, and use the following categories of personal information about you:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Gender
3. Job Title

6. How is Your Personal Information Collected?

We collect personal information about you through your onboarding as a BLOCKPHISH client, and as a result of and through our ongoing work for you. We also collect information through any submissions of information via the 'Contact Us' form on the website.

7. How We Will Use Information About You

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest [or for official purposes].

8. Situations in Which We Will Use Your Personal Information

We need all the categories of information in the list above (see paragraph 5) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

The situations in which we will process your personal information are listed in Schedule 1, together with the purpose or purposes for which we are processing or will process your personal information.

9. If You Fail to Provide Personal Information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as delivering an ethical phish), or we may be prevented from complying with our legal obligations.

10. Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

11. How We Use Sensitive Personal Information

"Special categories" sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about you in the course of legitimate business activities with the appropriate safeguards.

12. Do We Need Your Consent?

We do not need your consent if we use your personal information in accordance to carry out our legal obligations or exercise specific rights under the law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

13. Information About Criminal Convictions

We may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about you in the course of legitimate business activities with the appropriate safeguards.

14. Data Sharing

We may have to share your data with third parties, including third-party service providers and other entities in the business. We require third parties to respect the security of your data and to treat it in accordance with the law.

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. This may involve us sharing your information with:

1. Third party service providers who help us operate our business;
2. Organisations that introduce you to us;
3. Companies that we introduce you to; and
4. Companies you ask us to share your data with

If the make-up of BLOCKPHISH changes or such changes are proposed we may share your data with third parties to allow us to sell, merge or transfer aspects of our business or acquire or merge into other businesses. We will only do this if they agree to keep your data to the same standards we have set for holding your data. Following such a change other parties may use your data in line with these standards.

"Third parties" includes third-party service providers (including contractors and designated agents) that have a requirement to process your data for specific purposes. The third parties that process personal information are as follows:

#	System
1	Microsoft Office 365
2	Lucy Campaign Management
3	UKFast Hosting Provider

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

15. Data Security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Data Protection Officer.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

16. Data Retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Retention periods for your personal information are decided by considering the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. This will vary depending upon the relationship we have with you but in general terms for:

1. Business relationships we will retain your information for seven (7) years after the end of our relationship;

Personal information attributed to prospective clients that do not onboard with BLOCKPHISH is kept for no longer than is necessary. This will vary depending on circumstances but in general terms this will be a minimum of six (6) months.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

If you have any questions regarding data retention please speak to the Data Protection Officer.

17. Cookies

A cookie is a small data file that certain web sites write to your hard drive when you visit them. The only personal information a cookie can obtain is information a user supplies him or herself. A cookie cannot read data from your hard disk or read cookie files created by other sites. Cookies, however, enhance our web site performance in a number of ways, including providing a secure way for us to verify your identity during your visit to our web site and personalising your experience on our site, making it more convenient for you.

Our web site uses cookies so that we can serve you better. The site uses visitor tracking software that will use cookies to track information about how visitors come to the website, which pages they visit, and other actions that visitors make whilst on the site. This data is then used in order to improve the user experience of the web site. All user data collected in this manner is anonymous.

18. Rights of Access, Correction, Erasure, and Restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

1. Request access to your personal information (commonly known as a "subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

2. Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
3. Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
4. Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
5. Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
6. Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

19. Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

20. Changes to this Policy

We reserve the right to update this privacy statement at any time, and we will provide you with a new privacy statement when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Schedule 1 - How BLOCKPHISH Uses Your Data

How BLOCKPHISH uses client data	**Our basis for doing so**	**BLOCKPHISH's legitimate interests (where appropriate)**
To operate and maintain our relationship with clients	Your consent Contract fulfilment BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Developing and growing our business Obtaining your consent where needed for contact Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
Developing new service lines and products to better service clients	Contract fulfilment BLOCKPHISH's legitimate interest	Developing and growing our business Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
To learn how our clients' work with us and how we can improve this	BLOCKPHISH's legitimate interest	Developing and growing our business Obtaining your consent where needed for contact Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
To advise our clients about our services	Your consent BLOCKPHISH's legitimate interest	Developing and growing our business Obtaining your consent where needed for contact

Working with service providers who help BLOCKPHISH operate its business	Contract fulfilment BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Developing and growing our business Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
Designing and testing new products and services for our clients	BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Developing and growing our business Identifying the client base for our service lines Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
Delivering BLOCKPHISH's services to our clients	Contract fulfilment BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
Risk management	BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
Responding to complaints	BLOCKPHISH's legitimate interest BLOCKPHISH's legal obligations	Maintaining proper practice and efficiencies in meeting our legal and commercial obligations
To properly, efficiently and lawfully operate the business of BLOCKPHISH with proper regard to business	BLOCKPHISH's legitimate interest	Maintaining proper practice and efficiencies in meeting our legal and commercial obligations

planning and monitoring, internal communications and corporate governance, audit and oversight.	BLOCKPHISH's legal obligations	
To exercise BLOCKPHISH's contractual rights	Fulfilling contracts	N/A