GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 **Mobile:** 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

GDPR STATEMENT REGARDING BLINK OMS (11/05/2018)

GenerationNET Ltd takes data protection issues very seriously and aims to meet the regulatory requirements set out by GDPR. We would also like to assist our clients (users of Blink OMS) in ensuring that their business is managed in a GDPR compliant manner. This document aims to outline the GDPR issues and tasks that face a typical opticians practice based in Europe and offer 2 things:

1. An assurance that the Blink OMS system adheres to GDPR regulation and can assist your practice where this is concerned
2. Guidance towards other tasks that you may wish to consider

The following notes have been written to include advice based on the guidance issued by Optical Confederation – with specific reference to the document: http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance--final.pdf

In order to demonstrate GDPR compliance a UK optical practice should:

- have a written record of all data processing activities surrounding the identifiable personal information that they hold and use
- specify the legal basis under which they hold and process the data
- specify who the data will be shared with and for what reason
- review the methods used to keep the data secure
- review the consent process under which the data was obtained
- ensure that only essential data is collected and only stored for as long as it is needed
- allow the review, amendment, or deletion of personal data
- ensure that staff and anybody with access to the personal information can comply with the regulations

So GDPR compliance is more than just the Blink Optician Management Software system, however, Blink has been developed in a manner aimed to assist in keeping your patient data secure and to allow you to meet the regulations.

The lawful basis for storing data in Blink OMS

Note (taken from the Optical Confederation guidelines):

"Optical practices and businesses should NOT use consent as the lawful basis for processing health care records or staff records. This is because the conditions for consent are unlikely to be met." – using a lawful basis of consent would typically only be used for personal information about subjects who are NOT existing patients of the optical practice.

In the case of recording clinical data about existing patients (e.g. for patient records, retinal photographs, referral letters etc.) the lawful basis for processing patient data should be "Legitimate interest and for the purposes of health care". This reason does NOT require specific consent to be given by the patient, as long as the data is used for the purpose of health care and only kept for as long as necessary – 10 years according to the College of Optometrists.

In the case of recording dispensing and payment information, the same basis may be used, or it may be just for "Legitimate interest". The usage might be specified as; for taxation or accounting purposes.

Limited employee data is also stored within Blink (e.g. GOC number, email address) – this should be stored for "Legitimate interest".

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

How Blink OMS contributes to GDPR compliance

- Blink is designed for recording health information and dispensing/payment data for existing patients – as such, explicit patient consent is NOT required, follow up correspondence, appointment reminders and examination recalls are all legitimate uses of personal information
    - For clarification, it is expected that when patient information is exported into Blink, it is from existing patient records belonging to the practice using Blink
    - Despite recalls being a legitimate use of personal information on health grounds, patients can still opt out of recall correspondence, at the discretion of the practice, via the Lifestyle notes section of Blink
- The forms and methods used for recording patient data are constantly being improved in order to allow the highest quality of record keeping
- Blink allows referral letters and documents and system reports to be printed/stored and processed outside of the software system. It is up to the practice to ensure that this information is passed to the relevant body in an appropriate manner and/or stored securely or deleted as necessary
- Responding to Requests from patients – a patient is able to:
    - Request access to all of the information that is stored about them. Currently this information can be supplied by a practice through the taking of screen shots of the relevant data. GenerationNET can provide support to the practice in conducting this task, subject to availability and if a current support agreement is in place.
    - Request copies of prescriptions, receipts etc – these can be re-printed via Blink
- Correcting data – all patient information can be edited via Blink, it is the responsibility of the practice to maintain up to date information about a patient
- Deleting a patient – marking a patient 'Deceased or Deleted' via Blink DOES NOT remove the patient information from the system, it simply hides them from normal view and excludes them from typical recall procedures. This allows the practice administrator to view data concerning recently deceased/deleted patients
- Anonymising data – any patient who wishes to be 'Removed' from Blink can be anonymized. This will remove any identifying information from the system including the deletion of any uploaded attachments, however, the anonymous patient record will remain on the database for reporting/accounting purposes. This feature can only be used by an Admin user
- Report showing patients who have NOT been 'active' in the practice for a certain amount of time (i.e. since a given date) – these patients could then be anonymized at the discretion of the practice
- Audit Trail – Blink already records when users login to Blink but our audit trail has been improved to allow much more data to be recorded, including which patients are viewed or amended by a particular user and the ip address of the user at the time of access (audit data is stored for 7 days by default)
- Key data is encrypted before being stored. Some patient information stored on the Blink server is encrypted BEFORE being stored. This includes some address fields, email, telephone numbers and other identifying data. Note we cannot encrypt some fields including patient name and postcode because these fields are used to search for patients via the Blink interface and so need to remain in the database in plain text
- Data is encrypted via ssl before being transferred over https – as long as you see the padlock icon in your browser address bar you can be sure that any data transfer is secure
- Limited data exposure based on user permissions – Blink allows you to assign a 'type' to each system user. The user type restricts access to certain areas of the system, hence, preventing access to data to users who do not need access. The user types are continuously being reviewed.
- Secure system using strong passwords. Following the GDPR update, all users are encouraged to change their password, Blink will no longer allow weak or insecure passwords
- IP Address lockdown – although it can be very useful to access your patient records whilst on the move, do you really need to? If the answer is No and if your practice has a fixed ip address, we can lockdown your Blink system so that it is ONLY accessible via your practice network (or by Blink support staff)
- Regular backups & disaster recovery plan. Blink data is backed up remotely on a daily basis. We use a system called mozy.com for this purpose. All key files are uploaded to the Mozy platform, including database backups and patient file attachments. With regards to disaster recovery, we also manage a backup server which can be utilized if required. There maybe be some time required to bring the backup server fully upto date using the latest system backups etc, but once this is done we can then start to allow access to the backup server
- Data breaches – Blink aims to keep all users informed of server issues and data breaches

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

- Server kept upto date with patches etc – the server hosting the Blink system is a dedicated leased server hosted by ukhost4u (our backup server is a dedicated leased server hosted by 1and1). Access to the servers is available only to specific generationNET employees and relevant support staff at the host company.

Additional features available as part of the Blink 'Enhanced GDPR' System (please contact us if you'd like these features)

- For practices storing information about prospective patients, for direct marketing purposes, or for those sending out non clinical marketing material – there is a separate method of confirming that the patient has given specific consent for this kind of communication (which can be easily switched off). Note: marketing correspondence to existing patients may or may not require the enhanced GDPR system, for example, advertising the promotion of lenses designed to assist patients with a specific health requirement could be deemed as legitimate for the purpose of healthcare. Whereas, promotion of non-prescription lenses or optical accessories to all patients may not be legitimate. Therefore, Blink allows you to specify a patient's desire to be contacted in these cases.
- Responding to Requests – there is now a feature that creates a single pdf document containing all of the information stored about a patient. This document can be created at the press of a button
- Audit trail reporting. Without the enhanced GDPR update the Blink audit trail can only be accessed via Blink staff, taking the advanced update will allow each practice to create full reports on system access and usage, examining which member of staff did what and when it was done.
- Archive patients (bulk mode) – patients who have not been 'active' in the practice since a specified date can be anonymised

GDPR Features in Detail

Deleting a Patient using the 'Remove Patient' option will:

- Anonymise the patient by setting name, address etc to blanks
- Set DoB to 1/1/1900
- Delete all patient notes
- Delete all diary events linked to this patient
- Delete all medical info related to this patient
- Delete all freetext fields on the Lifestyle notes section
- Delete all documents linked to this patient including gos18s and all attachments stored on the server
- Delete record of any previous recall letters or SMS sent to this patient
- Delete all examination records, including recall dates
- Remove any data from freetext fields on the dispensing tables – records of sales transactions will remain on the system for finance accounting purposes

Stronger Passwords are now enforced. All staff members should be encouraged to change their passwords using the 'My Account' menu option when they next log into Blink.

Auditing is now much more comprehensive. Previously Blink would record every time a user logged in, now the actions listed below are all logged. System Administrator access to the event log is only available through the GDPR enhanced version of Blink, however, auditing still occurs on all versions greater the v2.51 and can be viewed by the Blink support team. On our standard systems audit records are kept for 7 days, on the GDPR enhanced version data retention is configurable.

Audited Actions:

- user login attempt
- password reminder request
- attempt to login from Invalid IP Address
- view patient info
- view patient details
- access data export
- view/edit staff admin
- add staff member
- view clinical info report
- view dispensing report

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

- view patient examination history
- view patient CL examination history
- view patient attachments
- view patient purchase history
- view patient medical conditions
- view patient lifestyle notes
- view patient document history
- start new full examination
- add new patient
- add new family
- add/edit diary appointment
- view appointment report
- view collections due or payments due report
- view payments report
- view collections report
- view order status report
- view voucher summary report
- start dispensing order
- view/edit dispense
- view dispense
- view lab info for a dispense
- update dispensing payment collection info

Note: the detail of which fields are edited is NOT recorded

Understanding what personally identifiable data is stored in Blink

Patient's personal & identifiable data includes:

- full name
- address *
- postcode
- telephone numbers (upto 3) *
- NHS number *
- Any free text stored in notes may be identifiable
- NI number *
- HC2/3 number
- Email address *
- Date of Birth
- Letter/images attached to Blink

Note: items marked with * are encrypted

Staff personal & identifiable data includes:

- full name
- username
- IP address (if accessing Blink from home)
- Email address
- GOC number

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

generationNET Ltd's own GDPR policy

For Blink OMS Clients:

All information is stored on the basis that we have a legitimate interest in doing so based on the fact that you are a Blink customer.

We store the following about you, your practice and your patients

- Practice name and contact information is stored in our accounting/invoicing system freeagent.com – we use this for invoicing or to contact you in a support capacity
- We hold information required to set up Blink for your practice, this can include data files from your previous systems passed to us so that we can import data into Blink – these will be deleted after use
- We hold email correspondence and notes used to provide you with an efficient and effective support service
- We store your name and email address in mailchimp, which we use for bulk emailing
- We store your patient database on our web server (as covered in the main body of this document) – this data will only be used/referenced for the purpose of supporting you in the management of your practice and your patients

Cloud based platforms that we use (which may hold some personal information):

- Mozy.com (owned by DELL) – for daily backups of our webserver and office based computers. All data is full encrypted, servers are based in Ireland (as far as we know) and a GDPR compliance document is available if needed
- UK Host For you – for our primary leased web server (Windows), our website hosting server (Linux) – this company is UK based, as are all the servers we use
- 1and1 – for our backup webserver (Windows) and also for our company email services and domainname registration – 1and1 is a global company with its origins in EU (Germany). Our backup Windows server is based in Germany. As far as we know our email services are managed on UK or German servers
- Freeagent – our invoicing system – this is a UK based company with servers here in the UK, data passed to the server is encrypted
- Mailchimp – our bulk emailing system – mailchimp is committed to GDPR and a policy document is available

Who we share information with (we only share information if it is required to perform a specific task):

- generationNET Ltd employees
- carefully selected freelancers (working on specific projects)
- technical support staff at any of our service providers listed above

We will not store or share information unnecessarily - once our use for the data has expired or you have not been a Blink client from more than 5 years we will endeavor to remove all data concerning your practice from our system

For Potential Blink OMS Clients:

All information is stored with your consent, following your interaction with our website (i.e. the form where you can 'Register Now' to 'Try Our Software') or following sales discussions. It is stored in our Mailchimp emailing system (mailchimp is committed to GDPR and a policy document is available) and it may also be stored in internal documents stored securely at our office.

We have recently cleansed our mailing list by requesting that historic contacts re-subscribe. Anybody who registers after April 26th will be added to our 'live' mailing list, but the process includes a 'double opt-in' feature and you have the opportunity to revoke consent any time.

Contact us

If you would like to know more about the information we hold about you please contact us via email to gdpr@blinkoms.co.uk or in writing to GDPR Team, Blink OMS, Bassett House, Main Street, Scraptoft, Leicester, LE7 9TD.

If you have a complaint about our handling of your data then you can contact The Information Commissioners Office (ICO)

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

Appendix I - GDPR Advice and notes taken from The Information Commissioners Office (ICO)

ref - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

What's new under the GDPR?

The documentation of processing activities is a new requirement under the GDPR.

You need to make sure that you have in place a record of your processing activities by 25 May 2018.

What is documentation?

Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this documentation.

Documenting your processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the GDPR.

Who needs to document their processing activities?

Controllers and processors each have their own documentation obligations.

There is a limited exemption for small and medium-sized organisations. **If you have fewer than 250 employees, you only need to document processing activities that**:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

What do we need to document under Article 30 of the GDPR?

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the GDPR and the UK's Data Protection Bill. Such documentation may include:

- information required for privacy notices, such as:
    - the lawful basis for the processing
    - the legitimate interests for the processing
    - individuals' rights
    - the existence of automated decision-making, including profiling
    - the source of the personal data;
- records of consent;
- controller-processor contracts;

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
    - the condition for processing in the Data Protection Bill
    - the lawful basis for the processing in the GDPR
    - your retention and erasure policy document.

How do we document our processing activities?

- Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.
- You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.
- When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

Appendix II - GDPR bullet points taken from the 100% Optical website

Ref - https://www.100percentoptical.com/news/industry-news-optical-insider/2462-gdpr-why-does-your-business-need-to-know-about-it?utm_medium=email&utm_term=&utm_content=READ%20MORE&utm_source=100%25%20Optical&utm_campaign=Gender%20differences%20observed%20in%20characteristics%20of%20dry%20eye%C2%A0%20%7C%20Optical%20Insider%3A%20Issue%2030

Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners – or face penalties for not doing so.

- **Communication**. A simple Privacy Policy that outlines what the data is you are going to collect and how you are going to use it, will no longer be sufficient. Within a Privacy Policy you will be expected to also explain your lawful basis for processing the data, your data retention periods and the statement that individuals have a right to complain to the ICO if they think there is an issue in how you are handling their data.
- **Holding Information**. The GDPR will require you to maintain records of all processing activities, and updates and changes to this need to be shared amongst your networking infrastructure, meaning anybody who you share data with needs to be made aware anytime updates happen such as erasures.
- **Increase of Rights for Individuals**. The GDPR includes the following rights for individuals: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making including profiling. Simply put, there's little that a subject can't demand to know about their data and what you're doing with it.
- **Lawful Basis**. The GDPR is firm that any company processing data has a lawful reason to do so. This means that you need to have a lawful purpose behind storing data, and this needs to be translated clearly on your Privacy Policy, and to any subjects who's data you hold.
- **Consent**. The GDPR contains firmer rules over what counts as consent to holding an individual's data. Consent must be freely given, specific, informed and unambiguous. There must be a procedure in place for the withdrawal of consent or of any amendment requests.
- **Children**. For the first time, the GDPR brings in special protection for children's data. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.
- **Data Breaches**. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. Organisations are expected to have this procedure in place in the event of a data breach.
- **Design & Data Protection Impact Assessments**. It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA), or Risk Assessment, as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'.

Access to your data. As well putting new obligations regarding collecting data, the GDPR is focused on giving the individuals whom data you hold more power. **When someone asks a business for their data, they must stump up the information within one month**.

==========

The ICO explained "you are expected to put into place comprehensive but proportionate governance measures," "Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place."

- **Storing Information**. You should document what personal data you hold, where it came from and who you share it with. This needs to be organised and clear.
- **Education**. Anybody processing data in your company needs to be educated about the GDPR and it's implications.
- **Privacy Policy**. You should review your current privacy notices and put a plan in place for making any necessary changes.
- **Individual's Rights**. You should check your procedures to ensure they cover all the rights that individuals have. This includes how you would delete data and how you would provide data, online and electronically.
- **Children**. Start thinking now whether you need to put systems in place that verify individual's ages and assess whether obtaining a parental or Guardian consent for any data your business holds is necessary.
- **Consent**. It's important to review how you seek, record and manage consent and whether you need to make any changes.

GenerationNet

Bassett House Main Street
Scraptoft Leicester LE7 9TD

Tel: 0116 292 7386 Mobile: 0776 481 5991
Email: info@generationnet.co.uk
Web: www.generationnet.co.uk

VAT Registration Number: 988 7369 32

- **Data Breaches**. Make sure you have the right procedures in place to detect, report and investigate a personal data breach.
- **Data Protection Officer**. Designate someone in the company to take responsibility for data protection compliance. Assess where how this role will sit with your organisation's structure and consider formal designation.
- **International**. If you operate in more than one EU member state (you carry out cross boarder processing) you need to determine your lead data protection supervisory authority.
- **Lawful Basis.** You should identify your lawful basis for the processing of the data you do. This is vital, as under the GDPR individual's rights will be modified depending on your claimed lawful basis for holding their information.
- **Design & Data Protection Impact Assessments**. You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.