BLW Data Protection Policy

1. RELEVANT CONTACT DETAILS INSIDE AND OUTSIDE BLW

Beacon Lee & Ward

8 Mantle St

Wellington

Somerset

TA21 8AW tel 01823 662234, lettings@beaconleeandward.co.uk

Data Controller (& Director): Jonathan Drew

Data processors: Rosemary Sykes Moore, Lucy Johnson, Jas Dyke, Sheena Grinter, Ruth Drew

Data protection officer: none appointed

Nature of business: residential letting agent

Company registration no: 4667171

Registered with ICO: Z7973339

BLW are committed to protecting your privacy and through this policy we set out how this is done.

BLW is a residential letting agent and so needs to collect and use limited personal data on adults with whom we serve or work with.

The Director and staff have an obligation to perform their duties for the proper management and governance of the business and to comply with regulatory requirements and ARLA licencing conditions.

The Director understands the need for privacy and we have a duty of care on how we handle and process individual client data. Information is stored in confidentiality and in accordance with legal provisions concerning data protection.

BLW does not sell, rent or otherwise deal in the personal information that we hold.

Third parties who process data for us

Rent4 Sure – for credit checks

TDS -for deposit logging

Third party book keeper providing accounting services to BLW

Contractors -for carrying out maintenance at rented properties handled by BLW

CFP Winman (Zoopla owned) - who supply and maintain our specialist letting software

1 TO 1 COMPUTERS who provide computer support

Rightmove – we just reply for a 'property info request' to the applicant

2. GENERAL DATA PROTECTION POLICY OVERVIEW

BLW have designed this 'Privacy by design' model, approved in April 2018 with the policy parts all becoming operational by 25.5.18 latest. Next review date is April 2019

BLW controls data on ' identifiable individuals' who include:-

current, past and potential tenants (& guarantors)

current, past and potential landlords (tf and managed)

BLW staff

Maintenance contractors- sole traders and companies

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

This policy exists to ensure that BLW complies with data protection law, protects the rights of staff, customers (landlords, tenants, guarantors)and maintenance contractors, that BLW is open about how it stores and processes individual data, and to protect itself from the risks of a data breach.

3. PURPOSES OF OUR DATA PROCESSING

BLW PERSONAL DATA CAPTURE

BLW data capture needs to be able to show compliance with the core GDPR principles

1. Lawfulness, fairness and transparency
2. Data only collected for specific purposes
3. Data minimisation
4. Accuracy and up to date
5. Storage limitation
6. integrity and confidentiality
7. accountability

1. Lawfulness, fairness, transparency

Landlord and Tenant data is given by each voluntarily to BLW with the intention of persuading the landlord/ applicant/ tenant/ guarantor to eventually agree & commence/ run a tenancy with appropriate communication until tenancy concludes and deposits balances are agreed at the end of the tenancy.

Only applicant/ tenant essential 'qualifying' data is sought from BLW , full names, contact names, information necessary to enable third party company to do credit check

Legally BLW must check tenants 'right to rent', take copy of passports

BLW need to be clear if tenants on benefits as some landlords have mortgages which do not allow them to rent to such cases

Landlord data- important to be clear on landlord name/ bank details for financial / tax / insurance reasons

Employees – necessity for performance of a contract, ie must have for contract of employment

And legitimate for the data controller to know employees

Contractor data- to qualify them as competent and insured, to give details of work and contact details of tenant/ landlord, to inform tenants of their names and contact details.

2.Purpose

To qualify tenants and then collect rent payments (for standing order or online transfer) by Agent (for managed) or Landlord (for tenant find)

To send financial statements, pass rent net payments to the landlord

To check landlord legally able to rent out, for ongoing communication during the tenancy

To check tenant is legally able to rent, for ongoing communication on the tenancy

To check contractors for competence and whether insured

3.Data minimisation

Landlord contact details- landlord or other contact points as given by landlord. Archive/ destroy after 6 years from tenancy end.

Tenant contact details, essential details for third party credit check, full name, contact details, no details on children names/ date of birth. Destroy applicants data after 12 months if no tenancy results.

4.Accuracy

Obtain details directly from tenants and landlords, names etc need to be correct on agency agreement and tenancy agreement, credit check on tenants, collect correct bank details, passport details for 'right to rent'

5.Storage limitation

Applicants looking for properties through Rightmove, hold for 3 months from receipt of email lead

During tenancy and then archive/ hold for further 6 years – landlord & tenant/ guarantor

Aborted tenancies – hold for one full year (ie could be up to 23 months)

Aborted applicants – hold for one full year (ie could be up to 23 months)

6.Integrity and confidentiality

Limited access – by staff member

Staff employment contracts- must keep 'client information' confidential

Third party contracts book keeper, credit checker signed agreements re GDPR

Proper archive disposal and shredding, to waste management company (keep receipts as proof).

7.Accountability

Each member of staff has some responsibility for ensuring data is collected, stored and handled appropriately– this is covered in an addendum to their work contract / in staff handbook

4. **DETAIL OF WHAT DATA PROCESSED**

Names and addresses, email addresses, phone data, bank info on tenants, landlords, prospective tenants, prospective landlords, contractors, other contacts (sometimes neighbours, relatives etc) -

contractors address and contact details, insurance certificates (for qualifying) – for sending out works orders, giving them property and or tenant/ landlord details

staff details - contact details, bank account details, NI number, c.v details - for initial appointment as employee, payroll, statutory requirements as employer

Full detail in our data audit

5. **HOW LONG DO WE PLAN TO KEEP THE DATA FOR**

live tenancies – ongoing, ad infinitum for tenant find ('tf') tenancies where deposits held and managed tenancies

contractors ongoing, for 6 years

archived, finished 'tf' tenancies for 6 years

archived finished 'managed' files for 6 years

diaries, day books current year and year before

aborted tenancies and applicants 1 year

6. **SECURITY – HOW DO WE PROTECT AND DOCUMENT THE DATA WE HAVE ?**

Protect

All 6 computers – By different password, each with AVAST firewall on each, which updates automatically

One server - OPNSENSE firewall is on server, this is configurable, everything can be excluded by default so nothing can get in, it does not need any maintenance. There is double ram memory on

server to accommodate this. The Windows 2012R2 server is located at back end of office, not identifiable.

There is still 'avast' anti virus software which sends updates to all machines.

Normally both the server and the berrys zoostoem machine must be left on . In the event of a power cut there is an auto restart.

The phone system works through the berrys router on marlena desk.

Use cfp new software to encrypt/ delate old records on landlords, tenants (contractors/ applicants)

2 rotated external hard drive back ups, one plugged in , other swapped each morning (keep one out of office at nights) 5-6 times a week.

There is no cloud storage, no lap tops so nothing taken out of the office apart from the one external hard drive back up disc.

CFP – each user has id and password, each staff member has different access to areas of software

Bank section - Director and book keeper only

Emails completed application forms typed, or scanned

Office archive – fully manned office in normal working hours, intruder alarm

(filing cabinets lockable for ' current ' managed)

No portable laptops outside office

CFP and 1 to 1 computers have RDP access to BLW for managing cfp software.

Document

By electronic system:-

Cfp runs back ups daily

Shared files – non cfp

By paper filing system :-

Managed current (with guarantor)

managed past (with guarantor)

tf current (with guarantor)

tf past (with guarantor)

keep past diaries

keep aborted tenancies

DISPOSAL

Paper filing

shred partly as we go along – blw own office shredder

shred hard copy pages, including tenant application form & copies of id, data given , guarantor,

old landlord – take to third party safe disposer (perrys recycling, brittania bridgwater)

Electronic

encrypt and delete old cfp records not needed after 6 years

7. PEOPLE, RISKS AND RESPONSIBILITIES

This policy applies to all staff at BLW and contractors working on behalf of BLW and it applies to all data that the company holds relating to identifiable individuals.

This policy helps to protect BLW from some very real data security risks including :

Breaches of confidentiality

Failing to offer choice to individuals on how BLW uses data held

Reputational damage – for instance if hackers gained access to sensitive data

Each member of BLW staff has some responsibility for ensuring data is collected, stored and handled appropriately in line with this policy. The only people able to access data covered by this policy should be those who need it for their work. BLW will provide training to all employees to help them understand their responsibilities when handling data. Employees should keep all data secure by taking sensible precautions and not disclose data to unauthorised people.

The Director of BLW is ultimately responsible for BLW meeting its legal obligations and reviewing this policy, arranging data protection training for staff, and dealing with 'subject access requests' from individuals. The Director is also responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards.

8. SUBJECT ACCESS REQUESTS

All SAR's must be treated individually, and firstly identify whether it is an SAR.

Often people may ask where their details are sourced from (their own supplied information on the application form or the credit check report) or just be given assurance that the data held won't be processed in future (ie for direct marketing purposes). These are not SAR's

If there is a formal request in writing (by email, letter) to be provided with all the personal data you hold , process on them, then you must treat the request as an SAR and currently have 40 days to comply.

When it is clear that there is an SAR the next thing to do is vital, that is to establish that the individual is who they say they are (or has rights to be applying for another person, such as a solicitor).

Staff need to recognise an SAR and know who to pass it to. The data controller (Jonathan Drew) is the person who should respond with the data.

The person requesting is only entitled to personal details on themselves.

If the data is no longer held, it does not need to be disclosed.

SAR comes from Section 7 of DPA

Subjects are allowed a copy of information held on them (to be sent electronically)

They can ask whether any personal data being processed

They can ask the reason it is being processed, and whether given to any other organisations or people

They have a right to know the source of the data

9. PROVIDING INFORMATION BY PRIVACY NOTICES

BLW aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights. BLW have sent out appropriate customised privacy notices to our existing landlords and tenants, staff, and contractors and will ask all new applicants (potential tenants) and landlords to sign consent forms in future.

Drafting and adoption of appropriate privacy statements in accordance with Art 13 to be used on collection or receipt of personal data (as blw own collection as data controller and by way of information processed from third party contractors), each BLW privacy statement to state

- identity and contact details of data controller
- purpose behind the processing of personal data and the legal basis for processing
- any legitimate interest relied on
- recipients or category of recipients of the personal data
- period for which data will be stored
- the right to request erasure or rectification of the data
- the right to withdraw consent
- the right to lodge a complaint with the ico
- whether the provision of data is a statutory or contractual requirement

- **10. BREACH POLICY**

- BLW keeps an internal processing and breach register
- BLW aims to learn from breaches and take any necessary remedial action
- BLW will treat 'Data breach' to include unauthorised access and alteration, not just data loss
- BLW will send a 'Reportable incident' to ICO within 72 hours
- Controller must inform subject when any breach detected
- Preparing for a data breach
- How to recognise
- We understand that a personal data breach isn't only loss of theft of personal data
- We have prepared a response plan for addressing any personal data breaches
- We have allocated responsibility for managing breaches to a dedicated person
- Our staff know how to escalate a security incident to the appropriate person
- **Responding to a personal data breach**
- Process to assess the likely risk to individuals as a result of the breach
- Notify ICO of a breach within 72 hours of becoming aware of it
- What info we must give ICO
- Process to inform affected individuals and advise how to protect from its effects
- We document all breaches even if don't all need to be reported

11. GDPR TRAINING FOR ALL STAFF

There will be personal training given to each member of staff based on flie with slides covering ;

GDPR language explained

BLW data protection policy overview

Purposes of our data processing

Details of what processed

How long data kept

Security/ disposal of data, paper and computer stored

SAR's - for staff awareness and preparedness

Privacy notices – explain relevance

Data breach policy

<u>Post training</u>

BLW Director will ensure that the 'output' result of training will be 2 part:-

Staff responsibility – produce customised draft typed sheet of GDPR responsibilities for each member of staff, agree, sign, date that training received

Each member of staff to have 'addendum' to employment contract that they will keep client information confidential in line with GDPR principles

April 11, 2018
