No Letting Go GDPR Policy and Risk Assessment

Definitions:

No Letting Go:	means No Letting Go, No Letting Go offices, Kaptur software or any third party company used by the group for processing information or hosting.
NLG:	means No Letting Go
KMS:	means Kaptur Management Suite and its third-party servers. This is the storage and management data base system where all No Letting Go and Kaptur reports are generated, managed and stored.
Kaptur	means Kaptur Management Suite or the mobile devices used to collect information from on site.
Clients	all customers of No Letting Go who provide personal data to fulfil the terms of our contract with you

Policy Statement

No Letting Go have taken steps to ensure that all personal data we collect falls in line with the GDPR regulations taking effect from May 2018.

No Letting Go collects personal information when you register with us or place an order for products or services. Personal information that you supply to us may be used in several ways:

- To allow us to fulfil the terms of our contract with you
- To provide information related to a franchise enquiry
- For statistical analysis
- For feedback on service levels provided

We will use this information to provide the services requested, maintain records and, if you agree, to send marketing information.

We will not disclose any information to any company outside the No Letting Go Group for any other reason unless required to do so by law.

For more information explaining how we use your information please see our privacy policy which is included in our terms of business, available via our web site – www.nolettinggo.co.uk or on www.kaptursoftware.co.uk

Policy Details and Procedures

NLG, our clients and our regional offices are all controllers of personal data.

Personal data (tenant and landlord information) is received by NLG, either directly into our management system (KMS) by the client or by other forms (works order, e mail, telephone etc.) and is inputted into KMS manually. This information is used solely by NLG to carry out the service we provide, including support and feedback. This is classified as "information necessary to fulfil the terms of a contract".

No Letting Go only hold personal information provided by clients, whether centrally or via regional offices within the KMS software system. We will hold the data for as long as is required to provide the contracted services, which will normally be until the end of a tenancy. No Letting Go policy is to delete all unrequired personal data.

Detailed information on how we manage and store data is listed below in policy details and procedures.

1. **Data and application storage.**

   All data is stored in the UK, through our third party host company on dedicated servers hosted by Rackspace in their LON3 data centre. This is a tier 1 data centre with 24 x 7 x 365 on site physical security, cctv monitoring and biometric and key card-controlled access to the server racks. The data centre itself is ISO27001, PCI-DSS and SOX compliant. Some data is temporarily stored and transferred through AWS (Amazon web servers), who are fully GDPR compliant.

2. **Data transfer policy**

   We do not transfer data between data centres outside of the EU or EEA.

3. **Data Protection Officer**

   No Letting Go have a nominated data protection officer and policies and procedures in place to ensure access to their customer's data is protected. For further information, please contact gdpr@nolettinggo.co.uk

4. **Data controls and risk management processes.**

   No Letting Go has a comprehensive secure development and data protection policy in place as well as a number of physical, procedural and software-based methods to protect any data hosted by our software processing partners. This includes

   - Dedicated firewalls which block all except essential ports from accessing our servers.
   - A process of regular automated scanning for security vulnerabilities by an accredited PCI Automated Scanning Vendor (ASV)
   - Ensuring that all access to our systems is performed over SSL using perfect forward secrecy where supported by the client web browser. Our SSL configuration is tested regularly using a third party SSL strength tester.
   - All remote access from our offices is performed over encrypted links.

- Our local network is configured with strong passwords and automatic lockouts
- All servers are configured with intrusion detection systems which track a number of suspicious events such as: remote logon outside normal hours, software installation, service modifications, etc.

stored only in our Kaptur Management Software system and personal information used for completing work activity is not used held outside of the system.

5. New Version Release Process

All changes to our software are released to a test system prior to release on the live environment to provide sufficient time to ensure that the changes function as requested and that changes to functionality have not exposed data that should not be visible.

6. Access to data

All technical and operational staff from No Letting Go have full access to the Kaptur software database so as to be able to resolve issues as requested. All clients have password protected logons to the Kaptur Management System with access to their information only.

7. Auditing security and technical measures on the protection of data.

We are happy to provide our clients with access to our data protection policy and if necessary, arrange for an audit at No Letting Go head office at the client's own cost.

8. Security breach notification process.

All production servers and our development offices are set up with a custom intrusion detection system that monitors a number of key events. These include

- Modification of firewall rules
- VPN access to the office
- Login to the production systems outside work hours
- Installation of software
- Updates to Windows Services
- Addition and modification of users and user groups

Upon detection of any of these events, our support team is immediately notified by email and will investigate. Windows event logs are expanded in size on all production systems to allow us to further investigate any potential breach and once the impact is known, clients would be notified immediately.

Staff or regional office staff are also required to notify the operations manager, DPO or technical director immediately if they think that any passwords or physical access tokens they use to access either production systems or our internal network have been compromised. This includes keys to the office, keycards for the office, network passwords and production server passwords.

9. NLG Password Policy

It is NLG policy to change passwords on a regular basis

10. Binding Corporate Rules

No Letting Go do not perform intra-organisational transfers of personal data across borders and as such do not follow Binding Corporate Rules.