

SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Agile Sports Technologies, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and Part 121 of the Regulations of the Commissioner of Education, as may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees, only to the extent that such actions are not already performed by Contractor as part of its security breach response process. Upon request, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

AGILE SPORTS TECHNOLOGIES, INC.

BY: _____

DATED: 06/03/2021

DATA SECURITY AND PRIVACY PLAN

CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.



Data Protection at Hudl

Hudl is a leading software company revolutionizing the way coaches and athletes prepare for and stay ahead of the competition. Hudl offers the tools to edit and share video, interact with stats, and create quality highlight reels for entertainment and recruiting purposes. The whole experience is available online, giving coaches and athletes secure access at home and on the go.

With more than 160,000 active teams and 4.3 million unique users, Hudl has become the preferred game film solution for all teams, from the smallest youth organizations to professional franchises in North America, South America, Europe, Asia, Africa and Australia.

Data is at the heart of what we do at Hudl and we handle a lot of it. In fact, we have 25 petabytes of data storage - that's the equivalent of 50,000 years of MP3s. And during the Autumn / Fall sports season, it isn't uncommon to get 35 hours of video uploaded per minute.

We've been looking after all this data since we were founded in 2006, and in that time we've gained the trust and long-term relationship of the biggest clubs, schools and leagues in world sport.

Our People

Hudl is a data driven company and so we bake security into everything we do. We structure our security expertise globally across the organization involving all parts of the business, including internal IT and Product Engineering.

Overall responsibility for Information Security at Hudl is with Brian Kaiser, co-founder and Chief Technology Officer, who leads all technical streams. Brian is a "hands-on" CTO and personally delivers in-person awareness sessions for all members of staff.



Data Protection and Privacy are led by Carl Gottlieb, Hudl's Data Protection Officer, who drives the data protection activities and training within Hudl.



Hudl provides ongoing internal Information Security and Data Protection training tailored to each specific job role, for which attendance and completion is tracked by Hudl's HR team

Hudl's hiring process is incredibly stringent, ensuring that only the very best and most trusted personnel can represent the organization. This includes extensive screening, testing, interviews and referral checking. All personnel including third parties are subject to strict Confidentiality agreements which form part of the contracts which are signed upon joining with Hudl.

Physical access to Hudl offices requires individually assigned secure door-entry badges, with staffed reception desks and video surveillance cameras in use. Data is stored within Amazon's AWS data centre buildings.

Our Processes

Hudl's Information Security Policy and Data Protection Policy detail the organization's approach to keeping data safe, private and under control. These internal documents are reviewed quarterly, made available on Hudl's intranet and used within internal awareness training. Hudl's website Privacy Policy can be found at <https://hudl.com/privacy>.

Hudl's Risk Management programme manages risks on a real-time basis with regular formal reviews, and critical issues acted upon immediately. We monitor our systems for vulnerabilities in underlying products and patch all critical vulnerabilities. Hudl follows its own internal security incident management processes and will notify the data controller without undue delay of any applicable incidents. Further details of data breach notification processes can be found within the customer's contract with Hudl.

Hudl's third party contracts comply with current data protection legislation and thus explicitly state the requisite levels of security within the service provision.



Our Technology

Hudl services and data are powered by Amazon Web Services (AWS). Hudl and Amazon are trusted partners and details of Amazon's Hudl case study can be found [here](#). Data is primarily stored within Amazon's US East (N. Virginia) "us-east-1" region and videos stored within Amazon regions close to the uploading origin. Whilst most of our servers are in the USA, we do have others located inside the E.U., as well as within Third Countries protected by EU approved Standard Contract Clauses. For more details about the security of these locations, see [here](#).



AWS has certification for compliance with ISO 27001, 27017, and 27018. These certifications are performed by independent third-party auditors. Details of Amazon's AWS ISO 27001 certification can be found [here](#).

Additionally, Amazon's AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. Amazon's SOC 3 report can be found [here](#). Amazon's SOC 1 (Type 2) and SOC 2 (Type 2) reports can be requested from [here](#).



Technical details of how Hudl manages its large AWS infrastructure can be found in our blog post [here](#).

Hudl encrypts data in transit, e.g. via TLS 1.3. Hudl plans to encrypt data at rest in the near future. Internal IT systems and products are tested on a regular basis and after major change.

Hudl utilises malware protection systems in multiple locations, including within email message flows and on workstations. Email content security solutions and other application aware systems help protect against data leakage. Firewalls and virtual private networks help secure access to Hudl's systems with more sensitive data placed in logical silos. All systems send logs to a single central analysis centre for monitoring and review.

Hudl's Software Development Lifecycle incorporates numerous levels of functional, non-functional and security testing.



Hudl's Business Continuity Policy is well established and primarily fronted by dynamic rerouting of traffic and load balancing within the Amazon AWS cloud. Failover scenarios are tested regularly, and due to the nature of the product architecture are delivered and tested at a micro-service level. Large scale systems such as DNS are dynamically scaled and failed over by Amazon. Hudl performs regular testing of its platform to ensure the data controller's service meets the agreed SLAs.

Your Privacy

Hudl is committed to strong data protection standards and has a dedicated Data Protection Officer based in the UK. Hudl stores data within Amazon's ISO 27001 certified data centres.

All data that Hudl sends out of the EU/EEA is sent to countries with an EU adequacy status or to organizations with signed EU Standard Contract Clauses. Hudl transfers data between its group of companies, for which the international transfers of EU/EEA data are detailed within Hudl's Intra-Group Data Transfer Agreement, which itself includes the required EU Standard Contract Clauses.

All Hudl data transfers to the US are TLS encrypted and generally consist of insensitive personal data. Hudl therefore believes the risk of government surveillance to the privacy of transferred personal data to be very low. Additionally, Hudl will only provide personal data to applicable law enforcement authorities when under strict legal compulsion. When permitted by applicable law, law enforcement and exigencies of time, Hudl will notify its customers of any such legal requests involving their personal data.

Hudl is primarily a data processor, and as such acts under the direct instructions of the data controller who maintains complete responsibility to establish a lawful basis for processing the data subject's data, e.g. that of an athlete.

Hudl's data processing meets its GDPR requirements and Hudl adheres to the six principles of lawful processing of Article 6 of the GDPR. Hudl's internal processes provide clubs with the ability to export, rectify and erase data should they need to service such a data subject request.



Hudl processes data on behalf of the club to provide the services. This data relates to the team, its athletes, their contact information, videos, photos, analytical data and messaging. This may include name, home and email addresses, phone number, school (name, city and state), graduation year, GPA, ACT/SAT scores, transcripts, parent/guardian information (name, relation, email and phone), age, birth date, photograph, height, weight, jersey number, Twitter handle, sports position, performance scores (40-yard dash, agility shuffle, power ball, vertical jump), speed and strength information, sports awards, sports videos featuring the athlete, and other athlete profile information.

Hudl retains customer data for the length of the service agreement with Hudl and as defined in the customer's contract.

Hudl provides Sportscodes software which provides local processing of data. No personal data is sent from the Sportscodes software to Hudl. In turn, Hudl itself does not process personal data of the club through this software product.

Hudl's website Privacy Policy is available at <https://hudl.com/privacy>.



Quick Facts

Company name and address:

Agile Sports Technologies, Inc (Hudl)
UK Office Address
Hudl UK, Ltd
Suncourt House 2nd Floor
8-26 Essex Road
London
N1 8LN
United Kingdom

Corporate HQ Address:

600 P Street
Suite 400
Lincoln
NE 68508
USA

Data Protection Officer (DPO) details:

| | |
|-------|--|
| Name | Carl Gottlieb |
| Email | dpo@hudl.com |
| Post | Data Protection Officer, Hudl UK, Ltd, Suncourt House 2nd Floor, 8-26 Essex Road, London, N1 8LN, United Kingdom |
| Phone | +1 402-817-0060 (Lincoln HQ number) |

EU Data Protection Authority Registration

Our UK subsidiary, Hudl UK, Ltd, is registered in England and Wales under registration number 06962812, with registered office at Suncourt House 2nd Floor, 8-26 Essex Road, London, England, N1 8LN. Hudl UK, Ltd is a registered Data Controller with the UK Information Commissioner's Office (ICO), number ZA326152.