

**IN THE MATTER OF PROCEEDINGS BROUGHT UNDER THE ANTI-DOPING RULES OF  
WORLD ATHLETICS**

Before:

Charles Hollander QC (Chair)

**BETWEEN:**

**World Athletics**

**Anti-Doping Organisation**

**and**

**Elena Orlova**

**Respondent**

---

**DECISION OF THE DISCIPLINARY TRIBUNAL**

---

1. The Claimant, World Athletics is the International Federation governing the sport of Athletics worldwide. The Respondent, Ms. Elena Orlova (the “Respondent”), is an Athlete Support Person under the Anti-Doping Rules (“ADR”) and is the Senior Coordinator for the Russian Athletics Federation (“RusAF” or “the Federation”), including acting as Team Leader for the Authorised Neutral Athletes from Russia who compete at International Competitions in Athletics.

## The allegations

2. This matter concerns a charge letter dated 21 November 2019 whereby the Athletics Integrity Unit (“AIU”) claims that the Respondent’s failure to comply with the IAAF Anti-Doping Rules (“**ADR**”), in particular, for
  - (i) failing to comply with the terms of a Demand issued to her on 17 May 2019 (“the **Device Demand**”) and
  - (ii) failing to comply with an Order of the Disciplinary Tribunal (“the **Order**”) issued in a Ruling dated 15 July 2019 (“the **Ruling**”) following the determination of an objection to the Device Demand filed by the Respondent, specifically for providing a different mobile telephone (or not the only mobile telephone) to that which was the subject of the Device Demand, to representatives of IB Group on 19 July 2019.

## Jurisdiction

3. The Tribunal has jurisdiction over this matter by virtue of Article 1.6 ADR. This was not contested.

## Investigation powers

4. Article 5.10 ADR provides the AIU with authority and jurisdiction to conduct investigations in accordance with the requirements of the World Anti-Doping Code and the International Standard for Testing and Investigations into matters that may evidence or lead to the discovery of evidence of anti-doping rule violations.
5. The ADR also provides the AIU with a number of investigative mechanisms to meet its duty to conduct investigations into potential anti-doping rule violations efficiently and effectively. This includes requiring Athletes and other Persons subject to the jurisdiction of the ADR to attend before the AIU for interview, to provide hard copy or electronic files and/or records and/or to provide any electronic storage device(s) that the Head of the AIU reasonably believes may have relevant information stored upon them that may evidence or lead to the discovery of evidence of anti-doping rule violations:

*“5.10.5 Without limiting the foregoing, pursuant to Article 5.10.4, the Head of the Integrity Unit may require an Athlete or other Person to:*

*(a) attend before the Integrity Unit for an interview, or to answer any question, or to provide a written statement setting out his knowledge of any relevant facts and circumstances;*

*(b) provide (or procure to the best of his ability, the provision by any third party) for inspection, copying and/or downloading any records in hardcopy or electronic format, that the Head of the Integrity Unit reasonably believes may contain relevant information (such as itemised telephone bills, bank statements, ledgers, notes, files, correspondence, e-mails, messages, servers);*

*(c) provide (or procure to the best of his ability, the provision by any third party) for inspection, copying and/or downloading any electronic storage device in which the Head of the Integrity Unit reasonably believes relevant information may be stored (such as cloud-based servers, computers, hard drives, tapes, disks, mobile telephones, laptop computers, tablets and other mobile storage devices).”*

6. Article 5.10.7 ADR provides the Head of the AIU with authority to request that any information, article, record or thing be provided to the AIU immediately, where the Head of the AIU reasonably believes that such items are capable of being damaged, altered, destroyed or hidden. The provision expressly provides that electronic storage devices or electronically stored information shall be deemed to meet this criterion and that the purpose for requiring such items to be provided immediately is in order to preserve the evidence that may be contained on them.

7. The recipient of a Demand under Article 5.10.7 ADR has a right to make an objection to a Demand by requesting a review by the Chairperson of the Disciplinary Tribunal within 7 days. However, the recipient’s right to submit an objection to the Demand does not obviate the requirement to comply with the Demand and immediately provide any information, record, article or thing to the Integrity Unit in order to preserve the evidence. Where an Athlete or other Person refuses or fails to comply immediately with a Demand, Article 5.10.7(b) ADR explicitly provides that the consequences in Article 12 ADR shall apply.

8. Article 7.8.4 ADR provides that the consequences in Article 12 ADR shall apply where an Athlete or other Person fails to produce the information, record, article or thing and any copy, or download of the same, following a determination by the Chairperson of the Disciplinary Tribunal (or his delegate) that there is a reasonable belief basis to the Demand:

*“7.8.4 Where the chairperson of the Disciplinary Tribunal or his delegate determines that there is a reasonable belief basis to the Demand, then if the Athlete or other Person fails to produce the*

*information, record, article or thing and any copy or download of the same, the consequences in Rule 12 apply."*

9. Article 12 ADR specifies that the Disciplinary Tribunal shall impose such sanctions as it sees fit, which may include a period of Ineligibility during which the Athlete or Athlete Support Person shall not be eligible to participate in Athletics:

**"ARTICLE 12 DISCIPLINARY PROCEEDINGS FOR NON-COMPLIANCE**

*12.1 Where an Athlete or other Person refuses or fails without compelling justification to comply with any provision of these Anti-Doping Rules, but such refusal or failure does not fall within any of the anti-doping rule violations defined in Article 2, the Athlete or Athlete Support Person shall not be deemed to have committed an Anti-Doping Rule Violation and he shall not be subject to any of the Consequences set out in Articles 9 and 10. However, disciplinary proceedings may be brought against him before the Disciplinary Tribunal in accordance with Article 8, and if the Disciplinary Tribunal finds that there has been such refusal or failure without compelling justification then it shall impose upon the Athlete or Athlete Support Person such sanctions as it sees fit (which may include, if it sees fit, a period during which the Athlete or Athlete Support Person shall not be eligible to participate in the sport)."*

**Factual background**

10. This is one of the cases arising out of the falsification of documents in respect of a Russian high-jumper Danil Lysenko.
11. The AIU opened an investigation into explanations advanced by Mr Lysenko ("the Athlete") for Whereabouts Failures (the "Investigation"). In the course of conducting the Investigation with the assistance of the Russian Anti- Doping Agency ("**RUSADA**"), the AIU discovered evidence that the Athlete had committed a violation of Tampering under Article 2.5 ADR by submitting false information and falsified medical documents to the AIU. On 10 April 2019, the Athlete attended an interview with representatives of the AIU in the context of the Investigation. The Athlete admitted that the medical documents submitted to the AIU in relation to the Whereabouts Failures were falsified medical documents and claimed that those falsified medical documents had been procured, produced and submitted with the assistance, aid, encouragement, conspiring, cover up and complicity of representatives of the Federation.
12. On 25 April 2019, the President of the Federation attended the offices of the AIU in Monaco for interview in the context of the Investigation and in accordance with a Demand for interview that

had been served on him by the Head of the Integrity Unit on 16 April 2019 pursuant to Article 15.8.4 ADR. During the course of this interview, the President of the Federation was issued with a Demand on the Federation (“the Federation Demand”), which obliged RusAF to:

- 12.1. provide (or procure to the best of its ability the provision by any third party) for inspection, copying and/or downloading, any records or files, in hardcopy or electronic format that the Head of the Integrity Unit believes in good faith may contain relevant information;
  - 12.2. provide (or procure to the best of its ability the provision by any third party) for inspection, copying and/or downloading, any electronic storage device (such as cloud based servers, computers, hard drives, tapes, disks, mobile telephones, laptop computers, tablets and other mobile storage devices) in which the Head of the Integrity Unit believes in good faith relevant information may be stored;
  - 12.3. provide passwords, login credentials and other identifying information required to access electronically stored records that are the subject of a Demand; and
  - 12.4. procure the full co-operation of its office holders, employees, servants, agents, consultants and contractors in responding to the Federation Demand.
13. Based on the findings of the Investigation, the Head of the Integrity Unit confirmed in the Federation Demand that he had formed a reasonable belief that:
- 13.1. relevant information may be stored on the e-mail and document servers of RusAF used between 31 March 2018 and 25 April 2019 (including cloud-based servers, hard drives, tapes, disks or other storage devices, including back-up tapes/disks/copies) (“the relevant e-mail and document servers”);
  - 13.2. relevant information may be stored on mobile storage devices and electronic communications devices (such as mobile telephones, tablets, personal computers, laptop computers, USBs and hard drives) that were the property of RusAF and used by any of the persons referred to in the Federation Demand (including the Respondent) in connection with their professional role between 31 March 2018 and 25 April 2019 (“the relevant devices”).
14. To facilitate the execution of the Federation Demand, the AIU arranged for representatives of RUSADA to attend the premises of RusAF to accept on behalf of the AIU the provision of the relevant e-mail and document servers and the relevant devices with the assistance of forensic imaging professionals in connection with the associated technical elements. The President of

RusAF, on behalf of the Federation provided his written consent to its execution. On 15 May 2019, the Head of the AIU wrote to the President of RusAF confirming that the Federation Demand would be executed on 16 May 2019 and facilitated by RUSADA acting with the assistance of forensic imaging professionals from IB Group in relation to the technical aspects of the Federation Demand. In the absence of the President of the Federation, the Executive Director of RusAF, Mr Alexander Parkin, gave a written undertaking that everything would be done to facilitate the implementation of the Federation Demand by RUSADA on 16 May 2019. At 10:00am on 16 May 2019, representatives of RUSADA attended the offices of RusAF in Moscow, Russia, accompanied by representatives of forensic imaging specialists, IB Group, to execute the Federation Demand on behalf of the AIU. Thus under Article 15.8.4 ADR, the Federation was obliged to provide (or procure to the best of its ability the provision by the Respondent) the Respondent's relevant devices.

15. Against that background, the Respondent provided access to a computer for inspection, copying and downloading pursuant to the Federation Demand, but she failed to hand over her mobile telephones on the basis that these were her personal property and did not belong to RusAF. She also raised concerns about her personal data and that of third parties stored on her mobile telephone and that any transfer of this data outside of Russia would result in a breach of Russian national law. In response the AIU proposed ("the Current Proposal") as detailed below:

- (i) at a mutually convenient date and time, under the full oversight and presence of the Applicant, a single image (copy) of her mobile telephone would be taken by representatives of IB Group using standard Cellebrite or Oxygen Forensics Detective imaging technology, or similar. The image would be sealed securely and would not be accessed, copied or duplicated;*
- (ii) at a subsequent mutually convenient date and time, the image would be accessed and examined by three persons, being (i) the Applicant, (ii) a RUSADA representative with knowledge of the case and an understanding of the information and evidence of relevance to the Investigation, and (iii) a representative from IB Group;*
- (iii) during this examination of the image, date restrictions and key word searches, numbers, phrases and images would be identified by the AIU (i) to reduce the propensity for irrelevant information to be accessed, copied or examined and (ii) to ensure that all information and/or evidence of relevance to the Investigation (including*

*any deletions or manipulations that may have been made by the Applicant) can be identified, isolated and copied into a case evidence folder; and*

- (iv) upon completion of the examination of the image, the case evidence folder alone would be preserved and placed onto a separate storage medium for viewing and downloading by the AIU as it considers necessary for the purposes of the Investigation;*
- (v) the original single image of the Applicant's mobile telephone (including all personal data contained on it) would then be stored securely to the satisfaction of the Applicant, the RUSADA appointed person and the representative of IB Group pending the outcome of the Investigation and any related disciplinary proceedings. The image would be sealed securely and would not be accessed, copied or duplicated without further order;*
- (vi) a full chain of custody and supporting documentation would be established for each step of the process described; and*
- (vii) following the completion of the process described, the Applicant's mobile telephone would be returned to her with all personal data on it left intact.*

16. The Respondent did not agree to the Current Proposal. She maintained that she would only give access to her mobile telephone under her supervision and control and to provide screenshots of relevant evidence and/or information (messages and e-mails) to be taken and forwarded to the AIU.

### **The Device Demand**

17. Thus the Head of the AIU issued a Demand to the Respondent on 17 May 2019 ("the Device Demand") pursuant to Article 5.10.5(c) ADR for the inspection, copying and/or downloading of her electronic storage devices, including, without limitation, the Respondent's mobile telephone(s), in the context of the Investigation. The Device Demand specified that the Respondent was to contact a RUSADA representative and present her electronic storage devices (including her mobile telephone(s)) for inspection, copying and/or downloading by forensic imaging professionals by no later than 13:00 Moscow Standard Time on the same date. The Respondent was also required to comply immediately, in particular, to preserve any evidence stored upon her electronic storage devices in accordance with Article 5.10.7 ADR.

18. The Respondent did not comply with the Device Demand. The Respondent's e-mail of 17 May 2019 asserted that she did not refuse to provide her personal mobile telephone, but that she had instead proposed to provide that telephone for checking and possible copying of relevant information in her presence and under her control on the basis that her personal mobile telephone contained personal, confidential information "*such as banking SMS and codes, passwords to various cards, personal messages to your relatives and friends, etc*" and because she wanted to "*see what is being copied and to control the process and to get 100% guarantees of protection*". Her 20 May 2019 e-mail provided further conditions, including that the Respondent would only provide access to her private e-mail account at her office computer in her presence and under her control for a search (not a full image) by key words and parameters and would only permit relevant e-mails to be forwarded or screenshots to be taken and access to her private (personal) mobile telephone for searching by key words and parameters in her presence and under her full control and for relevant information to be forwarded or screenshots to be taken. The Respondent failed to provide her mobile telephones for inspection, copying and downloading in accordance with the Device Demand, which could not be executed on 17 May 2019.
19. On 23 May 2019, the Respondent filed an objection to the Device Demand which stated the following:

*"I object to the Demand and request a review by the Chairperson of the Disciplinary Tribunal based on the following reasons:*

- 1. The Russian Constitution (art. 23) guarantees the right to the inviolability of private life, personal and family secrets; the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages.*
- 2. According to the effective Russian laws personal data may be disclosed only by a consent of the person whom these data relates to and it is strongly prohibited to give/disclose personal confidential information to third parties and to send it abroad (art. 6 of Federal Law "On Personal Data" N 152-FZ dated 27.07.2006).*

*Violation of these rules may entail civil, administrative and criminal liability provided by effective Russian legislation (art. 24 of Federal Law "On Personal Data" N 152-FZ dated 27.07.2006; art. 137 of Russian Criminal Code, art. 13.11 of Russian Code of Administrative Offences).*

*At my personal smartphone I keep:*



- my personal private and confidential information (including private pictures, private correspondence and notes) which is not related to my professional activities which I do not intend to disclose because of purely private nature of this information;

- sensitive financial information such as passwords from my bank accounts and other bank documents which are not related to my professional activities;

- most importantly, personal information related to my relatives, friends, acquaintances, who did not authorize me for disclosure of their personal information.

Taking into account the above I cannot violate the strict prohibitions provided by Russian **law** and do not intend to let copying my private information which is not related to my professional activities.”

### **Initial reference to the Disciplinary Tribunal**

20. Thus the matter was referred to the then Chairperson of the Disciplinary Tribunal. The Respondent submitted to the Tribunal that:

20.1. the Device Demand was unreasonable and disproportionate in the circumstances;

20.2. the Device Demand contradicted the mandatory rules of Russian law and fulfilment of the Current Proposal would result in severe negative consequences for the Respondent in Russia (including potential criminal liability); and

20.3. taking into account its contradiction to the Russian law regarding personal data protection, the Device Demand and the Current Proposal contradict the rules of the mandatory International Standard for the Protection of Privacy and Personal Information.

20.4. The Respondent requested that the Device Demand be set aside or adjusted in order that the Respondent could comply, but within the confines of Russian law.

21. On 15 July 2019, the Chairperson of the Tribunal, Michael Beloff QC, issued a ruling on the Objection filed by the Respondent (“the Ruling”). At [71], the Chairperson held that the single issue for his determination, i.e. whether there was a reasonable belief basis to the Device Demand, could not seriously be gainsaid:

“71. Pursuant to the Rules, literally read, there is only one issue for me to determine, that is to say whether there is a reasonable belief basis to the demand. If there is, it must be complied with by the person to whom it is directed; if there is not it can be ignored -indeed the AIU is not permitted

*to pursue it (although presumably if - unlikely as that may be - that person may voluntarily do that which the demand required).*

72. *If that were both the start and end of my enquiry there could be only one conclusion: the Applicant must comply with the demand. It is clear to me – and indeed it is not as such disputed by the Applicant - that the AIU has a reasonable basis for believing that the Applicant’s mobile telephone contains information which may evidence or lead to the discovery of evidence of an ADRV. That the AIU in point of fact entertains such belief is not-and cannot seriously be gainsaid. For my part I consider that such belief is reasonable on the basis set out in the next paragraph.*

73. *As the AIU stated in its Response:*

(i) *As was made clear in the Device Demand, the Athlete admitted in interview with the AIU that the explanation and medical documents for his Whereabouts Failures were forged and that the same were produced and submitted to the AIU with the assistance, aid, encouragement, conspiring, cover up and complicity of representatives of RusAF. Further, evidence obtained by the AIU, including from the Athlete and the RusAF President, indicated that the Applicant, along with other senior office holders, servants, agents or employees of RusAF, was either involved in an initial meeting to discuss the Athlete’s Whereabouts Failures or was involved in the process of provision of documents and/or explanations to the AIU, by or on behalf of the Athlete, in relation to his Whereabouts Failures or in communications regarding the same.*

(ii) *The Applicant has accepted in interview with the AIU that she was present at the initial meeting of RusAF representatives that was referred to by the Athlete.*

(iii) *The Applicant also accepts that she uses her mobile telephone for professional purposes.”*

22. The Chairman also dismissed the Respondent’s arguments in seeking to rely on what she contended to be superior law that limited the reach of the ADR including the Russian Constitution, Russian domestic laws on privacy and confidentiality as well as on principles embedded in the European Convention on Human Rights (privacy and property). The Chairman concluded that the Current Proposal was proportionate and ordered as follows (“the Order”):

“86. *The Applicant is required to comply with the Device Demand in the form of the Current Proposal within 7 days of the date of my decision or expose herself to the consequences set out in ADR Article 12”*

## Events after the Tribunal Ruling

23. On 16 July 2019, the AIU wrote to the Respondent and confirmed that the Objection had been rejected by the Chairperson of the Tribunal. The AIU requested the Respondent to confirm a convenient date and time between Tuesday 16 July 2019 and Tuesday 23 July 2019 on which she would attend the offices of IB Group to comply with the Order. On 17 July 2019, the Respondent replied to the Integrity Unit's letter of 16 July 2019 indicating that she was ready to comply with the Order, subject to "some reservations" as detailed below:

*"Hereby I am informing the Athletics Integrity Unit that:*

- 1. I sent the official request to the Public Prosecutor Office of the Russian Federation informing that I was demanded by the AIU to carry out activities that, from my perspective, may be regarded as administrative and criminal offences in Russia (as I previously stated in my Objection and Response);*

*I cannot take the risk of being prosecuted and punished in Russia and I will be able to comply with the Order only upon receipt of the official feedback from the Public Prosecutor Office of the Russian Federation which is empowered to prevent from violation of Russian law.*

- 2. Subject to absence of prohibition from the Public Prosecutor Office I will be able to provide the mobile as requested by the Order but I insist on being accompanied by my lawyer at all stages of the procedure.*
- 3. Please be informed that I am going on a business trip on Friday evening to another city in Russia to prepare and organise the Russian National Championships (overall organisation and coordination of such events is my main duty as RusAF staff member) and also to deliver lectures for athletics technical officials who are to officiate at the Russian National Championships (exact dates of the trip 19-28 July).*

*I will immediately inform the Athletics Integrity Unit about the official feedback from the Public Prosecutor Office and then will be able to agree timing and procedure of inspection of my smartphone."*

24. On 18 July 2019, the AIU replied to the Respondent's e-mail of 17 July 2019 and confirmed that she was obliged to comply with the Order, or otherwise (as provided in the Order) expose herself to the consequences in Article 12 ADR. The AIU confirmed that it had made arrangements on multiple dates for the Respondent to comply with the Order and invited her to attend the offices of IB Group in Moscow in order to do so. On 19 July 2019, the Respondent attended the offices of IB Group for the purpose of providing her personal mobile telephone(s) for imaging in accordance with the Demand and as required by the Order.
25. The Respondent provided a single mobile telephone Alcatel model 6037Y, IMEI 86469402209084 ("the Alcatel"). The Alcatel was handed to representatives of IB Group at

13:10 on Friday 19 July 2019 and an image of the Alcatel was obtained. The Alcatel was then returned to the Respondent on the same date at 18:30. However, during the imaging process of the Alcatel, amongst other matters, the Respondent disputed that she was required to provide log-in credentials for the purpose of accessing, inspecting and downloading information stored on any cloud-based servers that were linked to her personal mobile telephone that she handed over (including her e-mail account(s)).

26. The AIU wrote to the Respondent confirming that she was required to provide all passwords, login credentials and other identifying information required to access electronically stored records that are the subject of the Demand and clarified that this included all passwords and other credentials required to access information that is linked to her personal mobile telephone, including data stored on any cloud-based servers, such as those linked to her personal e-mail account. The Respondent replied by e-mail the same day and disputed that the Demand and the Order required her to do so. She maintained that she had provided her personal mobile telephone in accordance with the Demand and the Order.
27. On 16 August 2019, the AIU confirmed that the Respondent was required to attend the offices of IB Group in Moscow by no later than 23 August 2019 so that information stored on any cloud-based servers linked to her mobile telephone could be accessed, inspected and downloaded. On 22 August 2019, the Respondent attended the offices of IB Group in Moscow and provided login credentials so that the information stored on cloud-based servers (in particular those linked to her e-mail accounts with address [REDACTED] and [REDACTED]) could be accessed, inspected and downloaded in accordance with the Demand and the Order. On the same date, it was also agreed between representatives of IB Group, RUSADA and the AIU, that the image of the Alcatel obtained on 19 July 2019 and the information downloaded from any cloud-based servers on 22 August 2019 would be accessed and examined in accordance with [68](ii) *et seq.* of the Order on 28 August 2019.
28. The Device Data Report (“the **Report**”) provided by forensic imaging specialist of IB Group confirms the details of information retrieved during the examination of the image of the Alcatel pursuant to [68](ii) of the Order on 28 August 2019. This confirms that, at the time of imaging, the Alcatel was linked to the mobile telephone number [REDACTED]. In addition, the Report confirms that at the time of imaging, the Alcatel was linked to a WhatsApp account with the same mobile telephone number.
29. However, the AIU contends that this telephone number is not the Respondent’s personal mobile telephone number (or is not her only personal mobile telephone number) and therefore that the

Alcatel which she provided on 19 July 2019 is not the personal mobile telephone (or not the only personal mobile telephone) that she was required to provide pursuant to the Demand and in accordance with the Order.

30. According to the contact information retrieved from the Athlete's telephone during the course of the Investigation, the Respondent's personal mobile telephone number was stored with a different mobile telephone number [REDACTED].
31. In addition, the Respondent's mobile telephone number as stored in the Athlete's mobile telephone ([REDACTED]), was also entered (presumably by the Respondent) into the IAAF Event Entry System as the Respondent's contact telephone number in her role as Team Leader for the Authorised Neutral Athletes Team for the purposes of the recent IAAF World Championships in Athletics in Doha between 27 September 2019 and 6 October 2019.

### **The Respondent's Answer**

32. The Respondent provided an answer by way of written submissions. It contains an explanation of the facts relied upon by the Respondent and also analysis of Russian law. The Russian law set out in the brief was drafted by the Respondent's counsel, Mr Borodin, who is a qualified Russian lawyer.
33. The Respondent maintains in her brief that the arguments put forward by the AIU are "*not legally valid*" and submits that compliance with the Device Demand and the Order, "*create imminent and grave risks for the Respondent in Russia*".
34. The Respondent asserts through her brief that she eventually provided to IB Group her only mobile telephone and the AIU makes a mistake claiming that the Respondent had other telephones. In particular, the Respondent specifies that the Alcatel was the only relevant device that should have been provided for imaging in accordance with the Device Demand and the Order and therefore that they have been complied with. The Answer identifies the key issue for the Tribunal's determination to be "*the risk of criminal liability of the Respondent in case of fulfilment of the Device Demand and Order*".
35. The Answer also contends that the Respondent's smartphone contains various data of third parties of a private and personal nature (for example, photos and detailed correspondence regarding adoption of a child by a friend of the Respondent, intimate and personal messages, photos of minors and photos from the beach of the Respondent's friends (including alcohol

consumption), commercially sensitive information and contacts including those of Russian government officials.

36. The Respondent seeks to rely on the Russian Federal Law “On Personal Data” N152-FZ dated 27 July 2006 and Clause 1 of Article 137 of the Russian Criminal Code in order to conclude that the transfer of data as specified above in accordance with the Device Demand and the Order would be *“illegal under Russian law and will entail risk on criminal liability for the Respondent”*. The Answer also alleges that the AIU has failed to consider the rights of third parties over the data contained on the Respondent’s smartphone or the Respondent’s willingness to co-operate (i.e. to find a form of co-operation that would meet the objectives of the investigation in accordance with Russian law).

### **The AIU Reply**

37. The AIU led independent expert evidence on the application of Russian law. Mr Drew Holiner, who is a barrister in England and Wales, and is also a qualified and practising member of the Russian Bar. Mr Holiner has been instructed in proceedings at all levels of court in Russia and appeared in the courts of approximately a dozen regions of Russia. He also appears as an expert advisor or witness on matters of Russian and CIS law in proceedings conducted before foreign courts and arbitral tribunals throughout the world, including Armenia, the British Virgin Islands, the Cayman Islands, Cyprus, the Isle of Man, the Netherlands, New Zealand, the United Kingdom and the United States.
38. Insofar as the Respondent’s justification for failing to comply with the Device Demand related to alleged breaches of the Federal Law “On Personal Data”, Mr Holiner concludes as follows:
- 38.1. the Federal Law “On Personal Data” would not regulate the collection or submission of evidence in the course of an anti-doping investigation; and
- 38.2. even assuming that the Federal Law “On Personal Data” would apply to the Respondent’s circumstances, the legislation contains an applicable exemption that would permit the transfer of data (including sensitive personal data) on the Respondent’s smartphone in the manner set out in the Device Demand.
39. Moreover, in relation to the alleged risk of liability under the Russian Criminal Code were the Respondent to comply with the Device Demand, Mr Holiner concludes:

39.1. the Respondent's transfer of data under the Device Demand would fall within the scope of the exemption in Article 6 of the Federal Law "On Personal Data" and would therefore not be unlawful; and

39.2. even if there were no applicable exemptions justifying the transfer of data by the Respondent pursuant to the Device Demand, the information contained on the Respondent's smartphone would not qualify as a "personal or family secret" as set out in Article 137 of the Russian Criminal Code and its transfer would therefore not be unlawful.

40. Mr Holiner also concludes that the risk of any criminal (or administrative) prosecution or civil suit would have been further diminished by the terms of the "Current Proposal" as set out in the Order.

41. The Respondent contends that the Alcatel was her only mobile telephone.

42. The AIU maintains that the Respondent did not provide her only mobile telephone to IB Group when she provided the Alcatel on 19 July 2019.

43. The AIU say there is clear evidence that the Respondent was using a Sony Xperia smartphone in order to send e-mail communications directly from her e-mail address ( [REDACTED] ) to RusAF Executive Director, Mr Alexander Parkin, about the matter concerning Mr Danil Lysenko in May 2019.

44. The AIU say there is further evidence of the Respondent's use of a Sony Xperia Z smartphone in the Google Device Authentication information that was obtained by IB Group on 28 August 2019. In particular, this document provides that:

44.1. a Sony Xperia Z smartphone was used to access the Respondent's Google account on 18 August 2019 (using the Google Chrome browser on that device);

44.2. a Sony Xperia Z smartphone was last synchronised with the Respondent's Google account on 21 August 2019 at 21:12.

45. In addition, the AIU say there is further evidence of other mobile telephones (and other electronic storage devices including tablets) being directly authorised by the Respondent to access her Google account:

45.1. the Respondent authorised another mobile telephone, a Huawei P20 Lite smartphone, to access her Google account for the first time on 22 May 2019; and

45.2. the Huawei P20 Lite device was also used to access the Respondent's Google account on the day that Google Authentication information was obtained by IB Group on 28 August 2019<sup>1</sup>.

46. The AIU say the Respondent has failed to mention any Sony Xperia or Huawei P20 Lite smartphones in her explanations to date but rather asserts that the Alcatel was the only "relevant device".

47. Furthermore, the AIU asserts that the Respondent's explanations for her purchase of the Blackberry Keyone device are inconsistent. On 28 August 2019, the Respondent confirmed to representatives of IB Group that she had purchased the Blackberry Keyone device herself rather than it being presented to her by her mother as claimed in the Answer (see page 23 of the Transcript of the Respondent's attendance at IB Group on 28 August 2019):

*M: Let me check one more time, they worry about it there. The phone is the same that was before?*

*A: Let us see it.*

*EO: Sure.*

*A: We'll turn it on again and try it in other clouds, make sure again. We're not interested in a new phone, right?*

*M: What new phone? What do you mean by new?*

*A: Well, the one that the person is using now?*

*M: Ah, the new one?*

*A: After the last time it was the last day when this one was used, then-*

*EO: Well, it just doesn't work, it rejects the SIM card.*

*A: Yes, so-*

*M: The new or the old one?*

*E: The old.*

---

<sup>1</sup> The AIU also submits photographic evidence that appears to demonstrate the Respondent using another smartphone (as well as the Blackberry Keyone device referred to in the Answer) during the IAAF World Championships in Doha, Qatar, on 30 September 2019).



*EO: The old one. Its external speaker is dead, I told you last time.*

*M: And what is its model? Alcatel?*

*A: Alcatel.*

*EO: You copied it last time.*

*M: And another phone?*

*EO: Well, I just bought it.”*

### **The AIU case before the Disciplinary Tribunal**

48. The AIU contended that the Respondent has deliberately and repeatedly failed to comply with the ADR, in particular:
- a. for failing to immediately provide her electronic storage devices (including her mobile telephone(s)) for inspection, copying and downloading by the Integrity Unit in accordance with Article 5.10.7 ADR and the Device Demand on 17 May 2019 (“the First Failure”); and
  - b. for failing to comply with the Order as set out in the Ruling dated 15 July 2019 in accordance with Article 7.8.4 ADR by providing the Alcatel to representatives of IB Group on 19 July 2019, which was not her mobile telephone (or was not her only mobile telephone) that was the subject of the Device Demand (“the Second Failure”).

### **The Respondent’s case before the Tribunal**

49. The Respondent’s case was as follows:
- 49.1. She was entitled to refuse to comply with the Device Demand because she did not wish to act in breach of Russian law; in any event the Device Demand was superseded by the Ruling and subsequent events when she did comply.
  - 49.2. She was not in breach of the Ruling because she had no mobile devices apart from the Alcatel device.

## Discussion

50. The starting point is that the Respondent was obliged to comply with the Device Demand. The ADR require those subject to its rules to comply with legitimate demands; otherwise the investigation powers would be worthless. In a case such as the present, where a serious fraud had been committed in relation to the Athlete, it was of the utmost importance that the AIU's powers of investigation were not undermined. A refusal to comply obviously gives rise to an opportunity for tampering, particularly in a case where there had already been tampering.
51. As for the contention that Russian law prevented compliance:
- 51.1. This issue has been investigated and ruled on already in Mr Beloff's Ruling. I agree with his conclusions and analysis.
- 51.2. In any event, I do not accept that the Respondent is entitled to rely on Russian law as a reason for non-compliance. The Respondent has undertaken obligations under the ADR which are not governed by Russian law. Further, Russia has – as a Signatory of the UNESCO Convention Against Doping in Sport – enacted a Sports Law which provides for national anti-doping rules, which in turn require athletes and support personnel to comply with the anti-doping rules of inter alia International Federations such as World Athletics. Any processing would therefore be necessary to achieve the aims of an international treaty or law within the meaning of article 6(1)(2) of the Personal Data Law. World Athletics must be able to apply its rules equally to all athletes and other persons that are subject to them. If divergent national laws could be invoked, some athletes would be able to escape the investigatory powers of the AIU and others would not.
- 51.3. Further, I accept the evidence of Mr Holiner. To the extent that a contrary position has been put forward in the Respondent's case, oral evidence was not led to support it, and in any event I prefer Mr Holiner's evidence as independent. I do not consider that compliance would have put the respondent in breach of Russian law.
52. That leaves the second issue, namely whether the Respondent complied with the Ruling. The Respondent made herself available at the oral hearing before me to answer questions from the AIU. However, I reject her evidence that she had no devices other than the Alcatel. My reasons are as follows:

52.1. It is relevant at the outset to point out that the Respondent has not contested a four year ban for a tampering charge in relation to her involvement in the fabrication of documents in respect of the Athlete.

52.2. From the outset, the Respondent's stance has been to use every argument possible to avoid complying with the requirements of the AIU and their legitimate investigations. No device was handed over at all until 19 July, two months after the Device Demand. When the Respondent attended the offices of IB Group on 19 July 2019, she refused to provide login credentials for her e-mail and other accounts. This is despite the fact that she was required to *"provide passwords, login credentials and other identifying information required to access electronically stored records"*.

52.3. The Respondent claimed that she did not hand over her SIM card because it was not working at the time, and that she was not aware it contained stored data. She said that the Sony Xperia device (used by the Respondent to send e-mails on 6 May and synchronised with her Gmail account from 18 to 21 August 2019) belonged to her mother, although that was stated in evidence for the first time. She claimed she did not hand over the Huawei device because she only purchased it on 21 May, just after the period covered by the demand. That was also stated at the first time at the hearing.

53. As I said above, the Respondent has not contested a four year ban for her participation in the Tampering, which involved dishonest conduct on the part of all those involved. She has sought at every stage, both before and after the Ruling, to rely on every possible excuse to avoid compliance, and her excuses and justifications have changed significantly over time. It would have been easy, before and after the Ruling, to comply with the requirements of the AIU and to co-operate with the AIU. Her conduct, and her decision not to contest the Tampering charge, which of itself involves dishonesty, are consistent with a desire to impede the AIU, and give rise to the strong inference that she refused to co-operate in order to prevent the AIU having access to incriminating material. There is overwhelming evidence that what she presented on 19 July did not amount to full compliance with the Ruling. I am not prepared to accept her present justifications, noting particularly the fact that a number were put forward for the first time at the oral hearing, not supported by documentary material, and not consistent with what she had told the AIU previously.

54. In these circumstances I find that the Respondent did not comply with the Ruling. I therefore find both charges proved to the required standard of proof.

## Sanction

55. Where an Athlete or other Person refuses or fails to comply immediately with a Demand, Article 5.10.7(b) ADR explicitly provides that the consequences in Article 12 ADR shall apply.
56. In addition, Article 7.8.4 ADR expressly provides that the consequences in Article 12 ADR shall apply where an Athlete or other Person fails to produce the information, record, article or thing and any copy, or download of the same following determination by the Chairperson of the Disciplinary Tribunal (or his delegate) that there is a reasonable belief basis to the Demand.
57. Article 12 ADR provides the Disciplinary Tribunal with discretion to impose such sanctions as it sees fit:

### **ARTICLE 12 DISCIPLINARY PROCEEDINGS FOR NON-COMPLIANCE**

*12.1 Where an Athlete or other Person refuses or fails without compelling justification to comply with any provision of these Anti-Doping Rules, but such refusal or failure does not fall within any of the anti-doping rule violations defined in Article 2, the Athlete or Athlete Support Person shall not be deemed to have committed an Anti-Doping Rule Violation and he shall not be subject to any of the Consequences set out in Articles 9 and 10. However, disciplinary proceedings may be brought against him before the Disciplinary Tribunal in accordance with Article 8, and if the Disciplinary Tribunal finds that there has been such refusal or failure without compelling justification then it shall impose upon the Athlete or Athlete Support Person such sanctions as it sees fit (which may include, if it sees fit, a period during which the Athlete or Athlete Support Person shall not be eligible to participate in the sport).*

58. Where the CAS has had cause to consider 'failure to co-operate' offences, it is clear that such offences are considered to be of a serious nature, e.g. *Moon Joon Chung v. FIFA, CAS 2017/A/5086* and *Valcke v. FIFA, CAS 2017/A/5003*. The principle behind the investigative provisions of the ADR, including the requirement to provide electronic storage devices to the AIU immediately as set out in Article 5.10.7 ADR, is based on the need to preserve evidence of anti-doping rule violations and on the principle that those who are innocent have nothing to hide and, conversely, and by inference, that those who seek to hide something may have their reasons for doing so. In the absence of any coercive powers of investigation (such as law enforcement may have), the AIU is entirely dependent on the agreement or consent of an Athlete or Athlete Support Person to co-operate fully with the investigations that it undertakes.

59. That principle must therefore be rigorously observed and applied since a failure to do so undermines the very nature of the provisions themselves and the ability of the Integrity Unit to fulfil its mandate to protect the integrity of the sport of Athletics.
60. A person who fails to comply with the ADR in this way should not benefit from what would be a perverse situation if they were to benefit from a lighter sanction for non-compliance with the ADR than if an offence under the ADR had ultimately been discovered through an investigation successfully conducted by the Integrity Unit.
61. Where in this particular instance, the Investigation relates to potential violations of Article 2.5 ADR (Tampering or Attempted Tampering), which would lead to a mandatory period of ineligibility of four (4) years<sup>2</sup>, then a period of Ineligibility of at least four (4) years should be imposed on the Respondent for her failure to comply with the Device Demand and to provide her electronic storage devices.
62. These are serious matters and justify significant sanctions. I note that in *Ikkonikova* the Tribunal imposed an eight year ban and the cases might be regarded as similar. However, each case turns on its own facts and there is no suggestion in *Ikkonikova* that the Tribunal had in mind that the respondent would also be serving a further ban arising from the same incident.. Although the conduct here is separate, it arises out of the same incident. Whilst my jurisdiction is limited to these charges, I expect the sanction for these offences to be served consecutively with the sanction in relation to the Tampering charges. However, in considering what discretionary penalty is appropriate, it is relevant to have in mind that the Respondent will already be liable for a four year ban as a result of the Tampering charge and take what may be described as the totality principle into account in imposing a sentence for these offences.
63. In those circumstances, I will impose a six year ban for these offences in total, so that it is anticipated the Respondent will be liable to serve a total of ten years ban arising out of the events relating to the Athlete.

---

<sup>2</sup> Pursuant to Article 10.3.1 ADR

## Disposal

64. Based on the foregoing, the Tribunal finds:

- (i) that the Respondent failed to comply with the ADR, in particular:
  - a. for failing to immediately provide her electronic storage devices (including her mobile telephone(s)) for inspection, copying and downloading by the Integrity Unit in accordance with Article 5.10.7 ADR and the Device Demand on 17 May 2019; and
  - b. for failing to comply with the Order as set out in the Ruling dated 15 July 2019 in accordance with Article 7.8.4 ADR
- (ii) impose a period of Ineligibility of six years upon the Respondent pursuant to Article 12 ADR starting from the date of this Award.

65. I do not make any costs order.

66. This decision may be appealed to CAS in accordance with Article 13 ADR.



Charles Hollander QC

Chair

London

21 August 2020

1 Salisbury Square London EC4Y 8AE [resolve@sportresolutions.co.uk](mailto:resolve@sportresolutions.co.uk) 020 7036 1966

Company no: 03351039 Limited by guarantee in England and Wales  
Sport Resolutions is the trading name of Sports Dispute Resolution Panel Limited

[www.sportresolutions.co.uk](http://www.sportresolutions.co.uk)



ENABLING FAIR PLAY